

Comprehensive Guide on Information Systems Audit

© The Institute of Chartered Accountants of India
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior permission, in writing from the publisher.

First Edition: September, 2002

Second Edition: October, 2005

Price: Rs.500/-

ISBN No.: 81-88437-72-7

BMISA 541

E-mail: secyitc@icai.org

Website: <http://www.icai.org> & <http://isaicai.org>

Published for the Committee on Information Technology by
Ravi K. Arora, Secretary, Committee on Information Technology
The Institute of Chartered Accountants of India, ICAI Bhawan,
PO Box No. 7100, Indraprastha Marg, New Delhi - 110 002. INDIA

Printed by: Print Land, Delhi

Foreword

In the emerging scenario of global village and technological revolution, it is a challenging task for the Institute members to keep abreast with developments and convert threats into challenges and opportunities to grow in the globalised world. Increasing globalisation, business process outsourcing, need for Information Systems Security, IT penetration is impacting us in a big way. We now have greater competition and challenges. We not only have to provide quicker solutions but also provide value added services to businesses and regulatory authorities.

The Committee on Information Technology (CIT) has been established to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the threats and challenges ahead. Since its inception, the Committee has proactively considered the modern day requirements and initiated steps to suitably equip the members in terms of knowledge and skills to face the challenges ahead.

As businesses are increasingly using information technology solutions to service their core business functionality without having sufficient checks and balances leading to increasing business risks, there is increasing need for the Information System Assurance services or Systems and Process Assurance, as it is now being called, the Committee on Information Technology has introduced the Post Qualification Course on Information Systems Audit (ISA) to prepare the Chartered Accountants for this business opportunity.

I am glad to note that the Committee on Information Technology of the Institute has come out with this revised edition of the ISA Background Materials for the benefit of ISA Members with upgraded and enhanced content considering the revision and remodeling of course modules for the ISA Course.

I would like to place on record my deep appreciation for the efforts put in by Shri S. Gopalakrishnan, Chairman, Committee on Information Technology, Members of the Committee on Information Technology, the faculty members who have contributed the revised content and its Secretariat for this commendable job.

I wish you all the very best.

KAMLESH S. VIKAMSEY, President
New Delhi, September 16, 2005.

Preface

Today there is seamless integration of business processes, internal controls, accounting, systems and information technology. Our members need to provide increased assurance and other value added services to clients in this scenario.

The Committee on Information Technology (CIT) of ICAI established in the year 2000 to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the challenges ahead had started the course on Information Systems Audit (ISA) to suitably equip members to provide assurance related services in the field of Systems & Process Assurance and a course on Computer Accounting & Auditing Techniques (CAAT) to provide hands-on training on use of computers, CAAT Resources CD to provide exposure to use of General Audit Software/ Computer Assisted Audit Techniques. Additionally, the Committee has published the Technical Guide on Information Systems Audit to provide a guide to conduct of IS Audit and also organizes practical workshops/ Conferences/ Seminars to provide technical updates to members, apart from other developments.

The Committee on Information Technology is pleased to present this thoroughly revised, upgraded and enhanced Background Materials for the ISA Course keeping in view the required revisions to the course and modules in tune with developments in the field.

I am very thankful to Shri Kamlesh S. Vikamsey, President and Shri T.N. Manoharan Vice President, for the guidance and support in coming out with these revised materials. I would like to record my deep appreciation for the guidance and support of the Members of the Committee on Information Technology in coming out with the revised materials. I am also very thankful to all the teams involved in (a) conceptualizing the revision, (b) content/ material development, (c) content review, and (d) content editing/consolidation consisting of Prof. V. Janakiraman, Shri Nitin Bhawsar, Shri Mathew Thomas, Shri Rajendra Sardesai, Shri A. Rafeq, Shri Ananthasayana, Shri Mohan Bhatia, Shri S. A. Muraliprasad and Shri Deepjee Singhal, Shri.Vittalraj, Shri.Ramanathan, for this commendable job. I also acknowledge the significant contribution made by the Secretariat of the Committee, especially Shri A. Irudayam, Dy. Secretary, Southern Regional Office and Shri Ravi K. Arora, Secretary to the Committee.

I am confident that the revised Background Materials for the ISA Course will be of significant assistance to the members providing Information Assurance Services that is currently in increasing demand.

S. GOPALAKRISHNAN, Chairman,
Committee on Information Technology
New Delhi, September 8, 2005.

ISA Syllabus

Module 1: Information Technology Infrastructure

1 Introduction to Computer Hardware

Classification of Computers –Components of Computer–Data and Capacity Management–Selection Criteria for Hardware–Hardware Maintenance Procedures

2 Software Architecture

Classification of Software–Categories of Systems–Information Systems–Client – Server Architecture–Introduction to Object-Oriented Concepts–Stages in Software Development–The Selection Criteria for Software

3 Database Management Systems

Introduction–Roles and Duties of a Data Base Administrator–Data Base Failures and Recovery Procedures–Relational Model

Module 2: Communication & Networking Technologies

1 Introduction to Networking

Introduction to Networking–Classification of Networks–Types of Communication–Components of a Network–Network Topologies–The OSI Model–Networking Protocols

2 Network Hardware and Software

Network Cabling–Networking Devices–Network Operating Systems

3 Network Design and Maintenance

Principles of Network Design–WAN Technologies–Network Management–Data Backup and Recovery Strategies

4 Internet

Introduction to the Internet–Internet Infrastructure–Internet Services–World Wide Web

5 Network Security

Cryptography–Security Protocols–Firewalls–Intrusion Detection Systems(IDS)–Virtual Private Networks

Module 3: Protection of Information Assets

1 Introduction to Information Assets

Information Classification–Classification of Information Assets–Classification of Users–Naming Conventions–Access Control Models–Computer Crime–Computer Forensics

2 Information Security Policy

Tools to Implement Policy: Standards, Guidelines, and Procedures–Program Policy–Issue-Specific Policy–System-Specific Policy–Policy

Implementation–Interdependencies–Awareness, Training and Education–Cost Considerations–Audit of IS Security Policy

3 Logical Access Controls

Objectives of Logical Access–Paths of Logical Access–Logical Access Exposures–Access Controls and Authentication–Authentication Techniques–Access Controls in Operating Systems–Database Security–Audit Trail–Audit of Access Controls

4 Application Controls

Components of Application Controls–Application Boundary Controls–Input Controls–Processing Controls–Datafile controls–Output Controls–Existence Controls in Application Systems–Audit of Application Controls

5 Network Security Controls

Network Characteristics–Threats and Vulnerabilities–Network Security Controls–Auditing Network Security

6 Securing Physical Access

IS Assets: Objects of Physical Access Controls–Physical Access Threats and Exposures–Physical Access Control Techniques–Auditing Physical Access

7 Environmental Access Controls

IS Assets: Objects of Environmental Controls –Environmental Threats and Exposures–Techniques of Environmental Control–Administrative Controls–Technical Controls–Audit and Evaluation of Environmental Controls

Module 4: Systems Development Life Cycle & Application Systems

1 Business Application Development Framework

Need for Structured Systems Development Methodology–Overview of Phases in Structured Methodology of SDLC–Primary Phases in SDLC–Roles Involved in SDLC

2 Phases in Development of Software

System Design Phase–Development Phase: Programming Methods, Techniques & Languages–Software Testing Phase–Implementation of Software–Post Implementation Review–Umbrella Activities

3 Alternative Methodologies of Software Development

Data Oriented Systems Development–Object Oriented Systems Development–Prototyping–Rapid Application Development (RAD)–Reengineering–Structured Analysis–Web based Application Development–Agile Development–Information Systems Maintenance Practices

4 Project Management Tools and Techniques

Budgets and schedules–Gantt Charts–Program Evaluation Review Technique (PERT)–Critical Path Method (CPM)–System Development Tools and Productivity Aids

5 Auditing the System Development Process

IS Auditor's Role in Systems Development, Acquisition & Maintenance–IS Auditor's Role in Reviewing Developmental Phases of SDLC–IS Auditor's Role in Project Management

6 Specialised Systems

Artificial Intelligence (AI)–Expert Systems–Data Warehouse–Decision Support Systems (DSS)–Point of Sale Systems (POS)–Automatic Teller Machines (ATM)–EDI, E-Commerce, ERP Systems

Module 5: Business Continuity Planning

1 Introduction to BCP

Need for BCP/DRP–Types of Disasters–Steps in Developing a Business Continuity Plan–Law and Standards–

2 Risk Assessment

Objectives of Risk Assessment–Asset Identification and Prioritization–Threat Identification–Exposure (Vulnerability) Assessment–Specification of Objectives

3 Data Recovery

The Information Asset–Data Classification–Types of Backup–Technical Methods for Backup

4 System Recovery

Contingency Considerations –Strategies for Centralized Systems–Strategies for Networked Systems –Strategies for Distributed Systems–Strategies for Telecommunications Systems–Human Resources Issues

5 Contingency Plan Development

Components of an Effective Business Continuity Plan –Kinds of Plans–Insurance –Continuity Plan Organisation and Implementation–Testing and Validation–Business Continuity Plan Maintenance

6 Audit and Evaluation of BCP

Audit of BCP

Module 6: Information Systems Organisation & Management

1 Information Systems Organization & Management

Impact of IT and the Need for Related Competencies and Skill-sets–Business Process, Organization Structure and Controls –Corporate Governance and IT Governance–IT Steering Committee –IT Strategy Planning–IT Organization and Relationships–Segregation of Duties–

IT Policies, Procedures and Practices –Human Resource Management
–Key IT Activities–Auditing IT Polices, Procedures and Practices

2 IT Security and IT Security policies

IT Regulatory Issues–IT Security–IT Security Policy–IT Management
Issues–Auditing IT security and Controls

3 Information Systems Management and Controls

Management Responsibility –Categories of Control Techniques

4 IS Management Practices

Human Resource Management–Performance Management–
Documentation Standards–Auditing IT Management

5 IT Change Management

IT infrastructure Management–Configuration Management–Need
for Change and Change Management–Key Areas and Impact of IT
Change Management–Overview of Change Management Policies and
Procedures–Controls for Effective Change Management–Auditing IT
Change Management

6 Organization Structure & Controls in IT Department

Organizational Structure and IT controls–Management Structure–
Defining Roles and Responsibilities in IT department–Segregation
of Duties and Related techniques–Segregation of Duties–Identifying
Incompatible Functions–Information Access Classification–Auditing
IT Organization Structure and Controls

Module 7: IS Audit Process

1 Information Systems Risks and Controls

Information Systems Auditing Fundamentals–Information Security
– Fundamental Expectations–Information Systems Risk–IS Risk
Assessment–Understanding the Relationships Between IS risks and
Controls–Controls Assessment–Mitigating IS Risks Through IS Risk
Management –Role of Auditor in Risk Assessment–Audit Considerations
in Case of Outsourced –IT Activities–Information Systems Control
Framework–Security Policy Framework–IT Governance

2 Overview of Information Systems Audit

Impact of Information Technology on the Audit –Need for IS au-
dit–Definition of IS Audit–Fundamentals for Establishing an IS Audit
Function–Engagement Letter–Skills and Competence Requirements of
an IS Auditor –

3 Information Systems Audit Performance

Information Systems Audit Strategy–Phases in Information Systems
Audit–Planning an IS Audit–Audit of Outsourced Activities–
Materiality–Use of Sampling in Information Systems Audits–
Documentation Requirements–Reporting–Follow Up

4 IS Audit Techniques & Computer Assisted Audit Techniques

IT Environment Impact on Audit Methodology–Auditing in a Computerized Information Systems Environment–Audit of IT Controls and Security–IS Audit Approach–Computer Assisted Audit Techniques –Types of CAATs–Other Computer Assisted Audit Techniques–Continuous Auditing Approach

5 Overview of Information Systems Audit and Related Standards

Audit Standards–IS Audit Guidelines By ISACA–COBIT – IT Governance Model–Other Global Standards on IS Assurance and Audit–Overview of IT Certification –Overview of Regulatory Developments Impacting Controls in a Computerized Environment



Table of Contents

Volume I

Module 1:	Information Technology Infrastructure.....	1
1	Introduction to Computer Hardware	3
2	Software Architecture	17
3	Database Management Systems	35
Module 2:	Communication & Networking Technologies	55
1	Introduction to Networking	57
2	Network Hardware and Software	77
3	Network Design and Maintenance	95
4	Internet	115
5	Network Security	137
Module 3:	Protection of Information Assets	171
1	Introduction to Information Assets.....	173
2	Information Security Policy	187
3	Logical Access Controls	207
4	Application Controls.....	243
5	Network Security Controls	259
6	Securing Physical Access	293
7	Environmental Access Controls	305



Module 1: Information Technology Infrastructure

1 Introduction to Computer Hardware

✂ Learning Goals ✂

This chapter discusses the following topics:

1. Types of computers
2. Hardware architecture of the computer
3. Various Input/Output (I/O) devices
4. ASCII and EBCDIC codes
5. Hardware monitoring procedures
6. Data and capacity management
7. Hardware acquisition plan

After reading this chapter, one must be able to understand the working of a computer, various I/O devices and also the necessity of data and capacity management.

Introduction

A computer is an electronic device that performs high speed computation of data. Collins English Dictionary describes computer as ‘A device, usually electronic, that processes data according to a set of instructions.’ The actions carried out by the computer are either arithmetic or logical in nature. In this chapter, we discuss the architecture of a computer, classification of computers, various I/O devices that are in vogue.

Classification of Computers

Computers are either analog or digital in nature. Computers of the yesteryears were analog in nature but modern day computers are digital in nature.

Computers of today are generally classified on various factors:

1. Purpose for which they are built (general or special)
2. Size and data processing power they possess.

However, there is considerable overlapping in both these classifications.

Before we discuss the classification, let us briefly touch upon the history of computers. Computers of 1940's were vacuum tube based. They were large in size, consumed large quantum of power, very fragile and prone to breakdown. In late 50s, with the invention of transistor, size of

Module 1, Chapter 1

the computer systems reduced, speed of operations increased and they consumed less power compared to vacuum tubes. In 1960s, Integrated Circuit (IC) based systems came into the market. The IC based systems later evolved into Large Scale Integrated (LSI) circuit based systems, Very Large Scale Integrated (VLSI) circuit based systems and Ultra Large Scale Integrated (ULSI) circuit based systems. Computers of today are ULSI based.

On the basis of their processing power computers are classified as

1. Supercomputers
2. Mainframe machines
3. Mini Computers
4. Micro-computers or Personal Computers or Desktop machines
5. Notebook computers
6. Palmtop machines / Simputer

However, when we consider the purpose for which these machines are being built, the machines mentioned above can be used for general purpose. Also, there are machines which are specially built for specific purpose. Such as:

1. Engineering workstation
2. Graphics workstation.

Let us discuss about these machines in a detailed fashion.

Supercomputers

The largest, fastest and the most powerful computing machines are generally termed as supercomputers. They work on massively parallel architectures interconnecting more than one processor, has large quantity of main memory and secondary storage devices. They support multiple users, use proprietary hardware and software, need special environment for working and are very expensive in both procuring and maintaining. Supercomputers are usually used for complicated computations such as weather forecasting and other scientific research requiring massive calculations.

One typical example of a supercomputer is the Cray machine. In India, we have a supercomputer at Indian Institute of Science, Bangalore. The Pune based Centre for Development of Advanced Computing (CDAC) has also developed a supercomputer named Param. Param has been installed in several educational and research institutes in India.

Mainframe Machine

Mainframe computers are large and fast computers with powerful data processing capabilities. They are usually installed in very large organizations such as defence establishments, banks, meteorological offices where the volume of data to be processed is large. These machines, like

supercomputers support multiple users, have proprietary hardware and software. The cost of acquisition and maintenance of these machine are also high.

IBM is the most popular maker of mainframe machines and some of the models of IBM Mainframes are 3090, ES/9000, and S/390.

Mini Computers

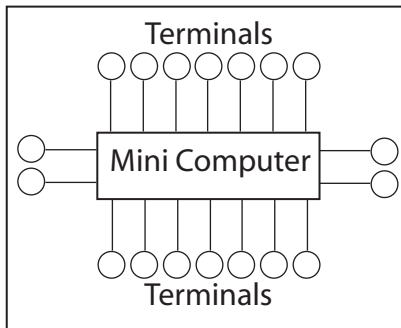
Mini Computer are scaled down version of mainframe machines. These machines are designed to meet the computing needs of small and medium enterprises (SME).

HP, IBM, SUN and Dell are some of the major vendors of mini computers. Mini computers support multiple users. The architecture of such machines is as follows.

There is a central machine which does all the computation. All users are connected to this machine either through dumb terminals (a terminal that does not do any processing, but merely collects data from the user and passes it on to the central machine for all processing) or through intelligent nodes. The total time of the central machine is shared among all the users.

Figure 1 shows the architecture of a mini computer. One of the most widely used operating system in mini computer is UNIX.

Figure 1: Architecture of a mini computer



Micro-computers or Personal Computers or Desktop machines

A Personal Computer, popularly called as a PC is a stand-alone machine based on a single microprocessor chip. These machines are single user systems. Many new features have been added to the PCs of today such as Digital Video Disks (DVD) and Liquid Crystal Display (LCD) Monitors. These are cost-effective machines which are used for general purpose computations.

Notebook Computers

Notebook Computers are lightweight machines which are more preferred by mobile users. These computers combine the advantages of a PC with mobility. A notebook uses flat-panel display. Because a notebook computer is used by a mobile user, these are equipped with battery back-ups. Typical examples of notebook computers are IBM Thinkpad, and Toshiba Protégé.

Palmtops

Palmtop machines are becoming more and more popular for they are extremely convenient to carry and offer features such as PIM (Personal Information Manager) that are needed the most by mobile users. One major problem faced by these machines is their small key boards and screens.

Some manufacturers are trying to solve the problem of small keyboard by replacing them with an electronic pen. Palmtops are also called Hand-held computers, Personal Digital Assistants (PDA) or Pocket computers. Figure 2 shows a PDA.

Figure 2: Personal Digital Assistant



Simputers

Simputer (Simple Computer), is an inexpensive, web-enabled handheld machine more powerful than a PDA. Figure 3 shows the picture of a Simputer.

Figure 3 The Amida 2200 Simputer



The simputer is slightly larger than a palmtop, runs on an Intel Strong-Arm chip that consumes low power, uses Linux operating system, and has a 32 MB of RAM, a screen of size 320x240, an internal modem, an infrared (IR) port, and a USB (Universal Serial Bus) port for connection to other devices. Details on Simputer can be had by sending an e-mail to simputer@csa.iisc.ernet.in.

Engineering & Graphics workstation

These machines are designed for the specialised purpose of engineering applications of CAD/CAM and other applications such as animations and multi-media. The main features of these machines are a powerful RISC (Reduced Instruction Set Computing) processor, high value of main memory, high resolution graphics screen and specialised software exclusively developed for this purpose. Sun, Apollo, Hewlett-Packard (HP), Silicon Graphics (SGI), Intergraph are some of the companies that make such workstations.

Components of a Computer

The components of a computer can be described by the functions they carry out. The computer mainly does the following four functions:

1. Receive data through input devices for processing.
2. Perform arithmetic and logic operations on the data received through the input devices.
3. Present the result of the computation to the users through output devices.
4. Store the information (both input and output) on secondary storage devices.

Figure 4 : Block diagram of a computer

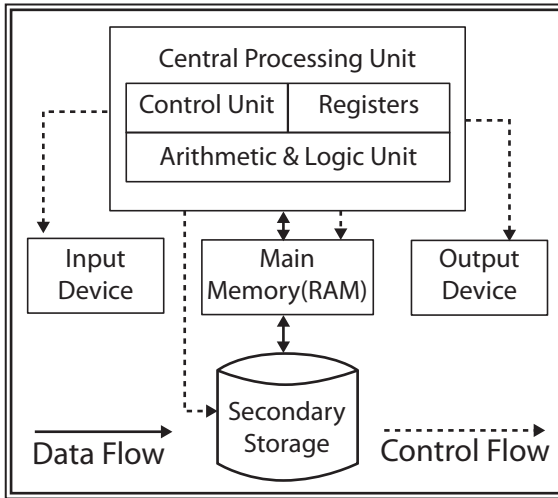


Figure 4 shows the block diagram of a computer. Description of various components is presented later. From the figure, it is clear that the main components of the computer system are:

1. Central Processing Unit (CPU) which consists of Arithmetic & Logic Unit (ALU), Control Unit (CU) and Temporary Storage units called Registers.
2. Main memory unit
3. Input devices
4. Output devices
5. Secondary Storage devices
6. Switch Mode Power Supply (SMPS) unit which supplies power to all these units.

Central Processing Unit (CPU)

The Central Processing Unit (CPU) is the core component of a computer. Housed in a ULSI chip called the microprocessor, it is this unit that carries out the arithmetic and logic operations at extremely high speeds, and controls the various operations of the machine. From figure 4, it is clear that the CPU has three main parts, the ALU, CU and Registers. The ALU unit performs the arithmetic operations (addition, subtraction, multiplication, and division) and logical operations (equal to, not equal to, greater than, not greater than, less than, not less than, greater than or equal to, not greater than or equal to, less than or equal to, not less than or equal to).

The CU controls the various input/output operations of the machine and instructs the system how to carry out the program's instructions. The CPU is driven by a 'clock' or pulse generator. Each instruction com-

pletes in a certain number of 'clock cycles'. Traditionally CPUs are based on CISC (Complex Instruction Set Computing) architecture, where a single instruction takes one or more clock cycles to complete. A new trend is to build RISC (Reduced Instruction Set Computing) processors which aim to be more efficient for a subset of instructions by using redundancy. These have simpler instructions but can execute much more quickly, sometimes with several instructions per clock cycle.

The CPU has some small quantity of memory for its own internal use. These hold the data and instructions temporarily during processing. This temporary memory present within the CPU is termed as Registers.

Typical examples of CPUs presently available in the market are Intel's Pentium processors, and AMD processors.

Main Memory or Random-Access-Memory (RAM)

Also called primary storage, it is this part that holds the data and instructions. Electronic and volatile in nature (means that when power is switched off, contents are lost) this memory operates at high speed that matches the speed of the working of the processor. All input and output devices communicate with this unit only.

Input/Output Devices

It is through the input devices that the computer system receives data for processing and through the output devices the results of the processing are presented to the user. These devices are mechanical or electrical or magnetic or optical in nature.

Table 1, 2 and 3 presents various details in Input, Output and Secondary storage devices.

Table 1: Input Devices

DEVICE	CHARACTERISTICS
Keyboard	Most widely used input device. Mechanical in nature. Available in 101 and 104 keys. Have the following basic types of keys – alphanumeric keys, modifier keys (Shift, Ctrl, Alt), special character keys, function keys (F1 to F12), Cursor movement keys (Arrow, PgUp, PgDn, Home, End), and special purpose keys (Ins, Del, Esc, Prt Scr, Scroll Lock and Pause).
Mouse	Also a popular input device. Mouse of yesteryears was mechanical in nature, presently they are optical in nature. Available in 2 button and 3 button models.
Trackball	Basically a pointing device. Mechanical in nature. One rotates the ball to move the pointer. Available in two button and three button models.

Module 1, Chapter 1

DEVICE	CHARACTERISTICS
Game Controllers	Used widely in computer games. Mechanical in nature. Typical examples are joysticks and game pads.
Scanner	An input device that scans text or graphics on a printed paper and digitizes the same into a form that computers can use. Photo-Electric in nature. Available in hand-held or flat-bed model.
Barcode reader	A device that reads the barcode printed and converts the same into a form that machine can understand. Has found wide acceptance in industry and in retail trade. Photo-Electric in nature.
Optical Character Recognition (OCR)	Reads text from paper and translates images into a form that computer can manipulate. Photo-electric in nature.
Digitizer	Helps one to feed drawings or sketches into a computer. Consists of an electronic tablet and a cursor or pen. By moving the pen on the electronic tablet, images are captured and processed later. Electro-mechanical in nature.
Voice Recognition	Helps in converting one's voice into digital form. Basically has a microphone, a set of speakers and appropriate software to identify the voice of the speaker. One of the most complex systems for there are lot of issues to be solved like Single user isolated word recognition, Single user continuous word recognition, Multi-user isolated word recognition, Multi-user continuous word recognition.
Web Cameras, Digital Cameras and Camcorders	Becoming more and more popular on account of Internet. These devices help in capturing still and continuous images in a digital form and transmitting the same.

Table 2: Output Devices

DEVICE	CHARACTERISTICS
Monitors	Popular output device. Electronic in nature. Available in two types, CRT monitors, used in all computers and flat-panel display systems used mainly in laptops and notebooks. Earlier we had monochrome monitors but today, they are seldom used. Important characteristics of a monitor are size of the screen, resolution, refresh rate, interlaced/non-interlaced, dot-pitch, and convergence.

DEVICE	CHARACTERISTICS
Printer	Yet another output device. Prints the output on paper or other media depending on the application. Classified as either impact or non-impact printer. Dot-matrix, daisy wheel, thermal and line printers are classified as impact printers, while inkjet and laser printers are classified as non-impact printers. Important characteristics of a printer are the quality of the output, speed of printing, type-impact or non-impact, capability to produce graphic images.
Plotter	Plotter is a device that produces drawings on paper, based on commands from a computer. Plotters differ from printers in that they draw lines using a pen. As a result, they can produce continuous lines. Multi-colour plotters are available today which use different-coloured pens. Plotters are more expensive than printers and are used mainly in engineering applications.
Sound cards and speakers	Sound cards help in converting digital signals into audio output which is then heard through the speakers. Today, with the advent of multi-media systems, sound cards and speakers have become integral parts of the computer.

Table 3: Secondary Storage Devices

DEVICE	CHARACTERISTICS
Magnetic tape	Most widely used secondary storage device for archival purposes. Data recording on tape and retrieval from tape, both are done sequentially. They have large storage capacities. Magnetic in nature. Acts as both input and output device.
Floppy disk	One of the most widely used secondary storage device, but losing its popularity due to unreliability of data storage. Magnetic in nature. Stores data in tracks and sectors. Has less storage capacity. Less expensive and portable. Available in 3.5 inches in size and has a capacity of 1.44 MB of data.
Hard disk	Has thin metal platter with iron oxide coating. Several such platters are mounted on a vertical shaft and spun at high speeds. Data is recorded and read using read/write heads on concentric circles called tracks. Has high storage capacities and is faster when compared to floppy disks. Magnetic in nature.

DEVICE	CHARACTERISTICS
Optical Disks	Optical in nature. Data is recorded and read using laser beams. Can store more data compared to hard disks. Available in three types – CD-ROM (Compact Disc – Read Only Memory), WORM disk (Write Once, Read Many) and CD-RW (Rewritable CDs). Today, optical disks are an integral part of any computer system. CD-ROMs have a storage capacity of 630 MB or more.
Digital Video Disk (DVD)	Similar to CD-ROM. Standard storage capacity is around 4.7 GB. But higher capacities are also available. DVDs are also available in DVD-R (DVD-Recordable) and DVD-RW (DVD-ReWritable) formats.
Smartcard	Yet another secondary storage that is becoming popular. Has an embedded IC on a card. Mainly used as an authentication device. However, other applications also use smart cards. Available in contact and non-contact types and as memory based and processor based. In memory based smart card, information once written cannot be erased and can only be read from it. Used mainly for authentication purpose. In processor based smart card, data can be written and read from the card. Typical applications include Voter's ID card, Patient Information, Digital Cash, Tax information, SIM card in cellphones.

Motherboard

Motherboard is the main circuit board of a microcomputer. The motherboard contains the connectors for attaching additional boards. Typically, the motherboard contains the CPU, BIOS, memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers required to control standard peripheral devices, such as the display screen, keyboard, and disk drive. Collectively, all these chips that reside on the motherboard are known as the chipset of the motherboard. On most PCs, it is possible to add memory chips directly to the motherboard. Figure 5 shows the picture of a motherboard with its various components.

Figure 5: Motherboard with its various components



Computer Codes

Codes are generally a form of representation. Computer codes help one to represent characters for use by the machine. The two main computer codes that are widely in use today are:

1. American Standard Code for Information Interchange (ASCII). This is the most prominent code for representing characters as numbers, with each letter assigned a number from 0 to 127. The standard ASCII character set uses 7 bits for each character. PC's use ASCII codes to represent data.
2. Extended Binary-Coded Decimal Interchange Code (EBCDIC). EBCDIC is an 8-bit code widely used on IBM mainframes. On account of being an eight-bit code, this permits representation of 256 characters.

Data and Capacity Management

In the present day and age, one of the main issues an organization has to face is the constant and never-ending growth of data and requirement for greater storage capacity. In addition to the data growth, the problem of data safety, security and integrity also need to be looked into.

In modern day enterprises which employ large scale database applications, multimedia applications, the requirements for disk storage runs from gigabytes to terabytes. If a proper data and storage management mechanism is in place, problems of downtime, business loss on account of lost data and insufficient storage space can be avoided.

The key issues addressed in data and capacity management include the following:

- ▶ How to effectively manage rapidly growing volumes of data?
- ▶ How to leverage data and storage technology to support business needs?

Module 1, Chapter 1

- ▶ What is the best data and storage management framework for an enterprise business environment?
- ▶ How to optimize the performance of the data storage hardware and software to ensure high availability?
- ▶ What is the best way to achieve greater storage capacity?
- ▶ How effective is the current data backup and storage management system?

Like every other investment in an organization, IT investments too need to be justified on Returns on Investment (RoI) basis. The capacity of IT resources required such as processor power, CPU clock speed, hard disk capacity and number of terminals need to be planned meticulously with business need in mind. Proper capacity planning has the following advantages:

1. It assures appropriate infrastructure capacity levels to support existing and future business functions.
2. It reduces resource expenditures and IT operating costs
3. It improve application infrastructure availability
4. It enables prioritization and reallocation of existing applications, systems, and network components.
5. It projects future resource needs, protecting the infrastructure from slow-downs as capacity demands increase.
6. It facilitates improved support of new and existing applications

Selection Criteria for Hardware Acquisition

Organisations need to be clear on their Information System requirements and what hardware and software have to be procured. In order to be unambiguous, it is essential to have a set of selection criteria for both hardware and software acquisition. Normally the hardware and software acquisition is done only after one carries out the data and capacity planning.

When one considers hardware acquisition, it is not merely limited to computers only but also to all equipment and peripherals associated with computer system such as printers, scanners, modems, routers, and CD-ROMs to cite a few. Before providing the specifications on what is needed to vendors in the form of an Invitation to Tender (ITT), it is essential to prepare a checklist based on the following evaluation criteria.

Compatibility and Industry Standards:

1. Is the hardware that is intended to be procured compatible with the existing one and takes care of future applications?
2. Have the workload and performance requirements been calculated and if done, is the hardware suggested capable of fulfilling it?
3. Are there any industry standards for the same and if so, do the hardware components comply with it?

Ease of Operation

1. Can hardware be installed and maintained by engineers available locally?
2. Can hardware be serviced, maintained, and upgraded locally?
3. Does the hardware need any special training for operations or will the users be able to access/use hardware with minimal additional technology competencies;

Support

1. What type of technical support will be provided by the vendor?
2. Are appropriate manuals for various operations available?
3. If so, are they available in a variety of media?
4. Are the manuals understandable for the intended users?
5. Does the vendor have a strong Research and Development Division with adequate staff?
6. Will the vendor help in smooth transition from the existing application to the new one?
7. What is the quantum of training the vendor will provide?
8. What is the backup facility the vendor will provide?

Cost

1. Is the cost quoted competitive and comprehensive?
2. Are all the requested components included in the purchase price?
3. Are there any hidden costs?
4. Will the vendor provide support at an affordable cost?

Hardware Maintenance Procedure

One of the important criteria that needs to be considered before finalizing the vendor is the issue of maintenance. The organization has to have a hardware maintenance program that takes care of this issue. The hardware maintenance program considers the following:

1. Which company takes care of what IT resource? For example, computer will be serviced by one company and printers by another.
2. How many times during a year does the vendor provide preventive maintenance and when?
3. What was the problem reported, if any, and what are the corrective steps? This has to be documented.
4. What is cost of maintenance? Has, at any time during the year, the amount spent for maintenance exceeded the budget? If so, the details and the reasons have to be documented.
5. Apart from preventive maintenance schedule, how many times during the year has the vendor come for servicing the equipment on account of failure?
6. What is the MTBF (Mean-Time-Between-Failure) and MTTR (Mean-Time-To-Repair) value? Typically MTBF value must be high and MTTR value must be low.

Module 1, Chapter 1

Hardware monitoring procedures aid in the hardware maintenance program. The following are the typical reports that are generated:

1. **Hardware Error Reports:** These reports provide details of failures, if any, of hardware resources in the organization
2. **Availability reports:** This report provides details on the availability of the hardware, software and all associated systems. IT division, being the life-line of the organization, the availability must be 24 X 365. If there is any break-down, this report provides details on the same.
3. **Utilisation Report:** All IT resources must be optimally used. If there is excessive utilization of a resource, steps have to be taken to correct it. Details on utilization parameters are automatically provided by tools supplied with the operating system and hardware. By using these tools, one can check the utilisation of CPU, memory, channel/bus, and hard disk.

These reports not only help in maintenance but also in effective planning for the future.

Summary

Computers are classified according to the purpose for which they are built and on the speed and capacity. Based on these, we have super-computers, mainframes, mini-computer, PC's, notebooks, PDAs and Simputer. Moreover we have specialized machines such as engineering and graphics workstation.

1. Various hardware components of the computer are presented. Details on CPU, Main memory, various I/O devices, SMPS and motherboard are presented.
2. Importance of data and capacity management is presented.
3. Selection criteria for hardware and software acquisition are discussed.
4. Importance and need of hardware maintenance program are emphasized.

References

1. Saunders D H, Computers Today, McGraw Hill International Edition, New York.
2. Leon A and Leon M, Introduction to Information Systems, Vijay Nicole Private Ltd. Chennai, 2004.



2 Software Architecture

✂ Learning Goals ✂

This chapter describes software architecture. The topics covered in this chapter are:

1. Definition of systems and application software
2. Various systems software and its brief description
3. Operating systems and its functions
4. Generations of programming languages
5. Client-Server Architecture
6. Introduction to Object-oriented concepts
7. Types of Information Systems
8. Stages in software development and change control procedures

After reading this chapter, one must be able to understand the importance of software, how operating systems and other associated systems work.

Introduction

If one wants to get their jobs done by the computer, they need appropriate software and data. In this chapter, we discuss on the software concepts and types of information systems. Moreover, stages in software development are also presented.

Classification of Software

The term software in a broader sense refers to the program that the machine executes. There are two broad classification of software:

1. **Systems Software:** These refer to the set of programs that:
 - a. Enables the computer to work
 - b. Control the working of the computer
 - c. Provide facilities for programmers to develop application
 - d. Enables various I/O devices to be connected; and
 - e. Helps in efficient use of the computer resources.

There are various categories of systems software. They are Operating Systems, Programming languages, Device drivers, and Utilities. A brief description of these is given below.

2. **Applications Software:** Refers to the set of software that actually does the job for the end-user. There are innumerable application software that is available depending on the need of the user.

Operating Systems (OS)

Any computer has four important resources. They are RAM, CPU, various I/O devices (which include secondary storage devices also) and the information that is held in the machine. All these resources have to be scheduled to various users whenever they want. This is done by the operating system. Hence one apt definition for an OS is **RESOURCE MANAGER**. OS enables users to interact with the machine and takes care of technical aspects of a computer’s operation. It shields the user of the machine from the low-level details of the machine’s operation and provides frequently needed facilities.

There are various types of operating systems:

- 1. **Single-user OS:** Here, only one user can use the system at a time. The number of processors is usually one.
- 2. **Multi-user OS:** Here, several users can use the system simultaneously. Here also, the number of processors is usually one.
- 3. **Multi-processing OS:** Here, the OS operates on a system that has more than one processor.
- 4. **Real-time OS:** Today, embedded systems are being extensively used in various applications. Embedded systems are application-specific computers. Embedded systems employ a combination of hardware and software techniques to perform a specific function. The application areas include household products (toasters, cooking ranges), consumer electronics (handheld gizmos, cell phones, game machines, MP3 players, smart cards), automobiles (antilock brakes, noise reducers), office products (printers, fax machines) and Internet infrastructure (chips for network infrastructure, VoIP). These embedded systems use a real-time operating system (RTOS) to carry out their tasks. An RTOS schedules a small set of tasks with demanding and precise response time requirements. Micro C/OS-II is a typical example for RTOS.

Two more concepts need to be discussed in conjunction with the above. They are: single tasking and multi-tasking. In a single-tasking OS, only one application can be run at a time. In a multi-tasking OS, more than one application can be run. It is obvious that a multi-user OS has to be multi-tasking OS. Table 1 gives examples of various types of OS.

Table 1: Examples of various types of OS

OPERATING SYSTEM	SINGLE/MULTI-USER	SINGLE/MULTI TASKING	NO. OF PROCES- SORS
MS-DOS	Single User	Single -tasking	One
Windows 9x	Single User	Multi-tasking	One
UNIX	Multi-User	Multi-tasking	> 1

OPERATING SYSTEM	SINGLE/MULTI-USER	SINGLE/MULTI TASKING	NO. OF PROCES- SORS
Windows 2000	Multi-User	Multi-Tasking	> 1
Linux#	Multi-user	Multi-tasking	> 1

(#Unix is one of the most important operating system today and it comes in many flavours, developed by different manufacturers. Linux is a version of Unix and its source code is now available in the public domain)

Core Tasks of an OS

The core tasks of an operating system are:

1. **Processor management** - Controls processes and access of CPU by applications so that each has its fair share of the CPU time.
2. **Memory management** – Manages the RAM allocation to various applications. It also manages virtual memory and paging.
3. **Device management** – Manages various I/O devices connected to the system. Takes care of the problem of disk scheduling.
4. **Information Management** – Manages the information that is stored in the machine. Information is stored in the computer in the form of files and databases. The system must provide facilities to users to create, access (both complete and restricted), delete, rename, modify and save them. In order to do these activities, an OS provides facilities at various levels. At the lowest level, an OS interacts with the device drivers (provided by the manufacturers of the devices) of devices such as tape and CD-ROMs. The next level is the basic file system which is concerned with placement of data on these devices. The basic file system interacts with the file management system. File management system mainly deals with file organization and access methods. The common file organization methods are sequential, indexed-sequential, indexed, and direct. Data is stored in one of these methods and is accessed accordingly.
5. **Application Interface** – Provides Application Program Interfaces (APIs) to various software.
6. **User interface** – Providing appropriate interfaces for the user to communicate with the system.

The core tasks of processor management, memory management, device management and information management are implemented in the kernel of the OS. The kernel, which deals with the basic system resources, is the core of an operating system. The kernel drives physical devices and handles I/O, memory management and process scheduling.

The basic structure of any OS has two layers – the kernel and the shell. The hardware is surrounded by the kernel. It is only through the kernel that communication with the hardware can be established. The kernel

Module 1, Chapter 2

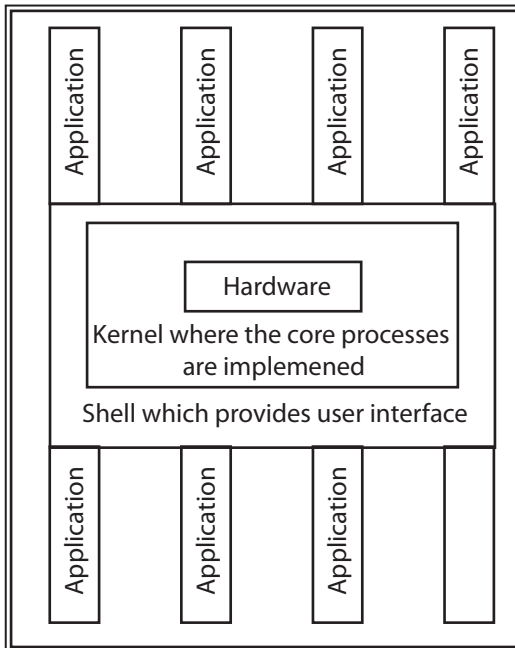
is surrounded by the shell which provides the interface for various applications. Application programs run over the shell. Figure 1 shows the structure of an OS.

Major functions of a Kernel

The major functions of a kernel are:

1. It controls and mediates access to hardware.
2. It schedules / allocates system resources of Memory, CPU, disk, etc.
3. It enforces security and protection.
4. It responds to user requests for service (system calls).

Figure 1: Structure of an OS



OS generally operates in two modes:

Supervisory mode: In this privileged mode, the user has full and complete access to all the resources of the computer bypassing all security features. Hence, this state must be operated with extreme caution.

Restricted or General User mode: In this mode, a user can access only those resources for which rights have been granted. Normally all users are allowed to operate only in the general user mode. If the user wants to perform some privileged functions, they must communicate with the code running in the privileged OS area.

Stallings [8] provides more details on the working of operating systems.

Programming Languages

Computer programming languages help a programmer to communicate with the computer. These programming languages have evolved through various phases or generations. The various generations of languages are:

First-Generation Language (1GL): Also called machine language, instructions to the computer have to be provided in a string of 0s and 1s.

Second-Generation Language (2GL): Also called Assembly Level language, here instead of 0s and 1s, mnemonics and operation codes (op-codes) are used.

Third-Generation Language (3GL): Also termed as procedure-oriented language; instructions are given in a structured way that resembles English language. On account of this, humans can understand what the program does and what the logic of the program is. The main characteristic of a 3GL is that one has to tell the system what to do and how to do.

Fourth-Generation Language (4GL): Also termed as database languages or report generators. Here, the user specifies the problem in a very general fashion and leave the computer to provide a solution. In other words, one has to only tell the system what to do. The “how to do” process is taken care of by the computer itself.

Fifth-Generation Language (5GL): Technically, 5GL have a natural language interface to it. Here, the inquirer inquires the system in their own natural language. This falls within the ambit of Artificial Intelligence (AI) and Natural Language Processing (NLP). Extensive research is being carried out in these areas.

Assemblers, Compilers & Interpreters

A computer system will understand instructions and execute the same, when it is presented as a sequence of 0s and 1s. However, humans do not write computer programs in 0s and 1s but in higher level languages. Hence, the program has to be translated to machine code. There exist various translators that help in converting programs written in higher level language into machine code. Assemblers, compilers and interpreters are such translators. Table 2 provides the major types and functions of these translators.

Table 2: Major types and functions of translator

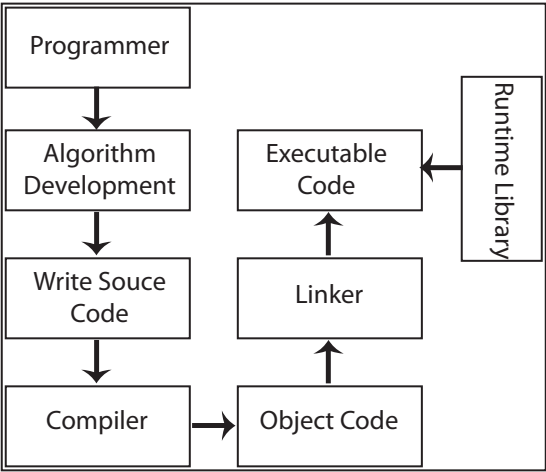
TRANSLATOR	FUNCTION
Assembler	Takes an assembly level code as input and produces corresponding machine code as output.

TRANSLATOR	FUNCTION
Language Compiler	Takes a 3GL code as an input and produces corresponding machine code as output. A compiler takes a program as a single unit, compiles the same, checks for errors and if error-free, produces machine code as the output. For every programming language, there are one or more language compilers.
Language Interpreter	Similar to a compiler, an interpreter takes a 3GL code as an input and produces corresponding machine code as output. Unlike a compiler, an interpreter translates each program statement into machine code just before the program statement is executed. Main advantage of an interpreter is that it is easier to debug programs using an interpreter. However, programs are executed slowly when compared to compiled programs.
SQL Engine	A translator that takes a SQL statement as the input and produces corresponding machine code.

Compilation Process

The process of compilation is depicted in figure 2.

Figure 2: Compilation process



Device Drivers

These are a part of the system software which informs the computer how to use a particular peripheral device such as a printer or CD-ROM. Normally, the device drivers are supplied along with the device and one has to install them in the machine.

Linker

Linking is the process of combining various pieces of code and data together to form a single executable unit that can be loaded in memory. The process of linking is generally done during compilation of the program. After linking, loading process takes place which is done by loader software.

Loader

A loader is a program, which loads the code and data of the executable object file into the main memory, goes to the very first instruction and then executes the program.

Debugger

A debugger is a utility that helps in identifying any problem occurring during execution. Using the debugger utility, one can pinpoint when and where a program terminates abnormally, show the value of the variables used, and in general provide information so that the programmer, can locate bugs.

Editor

An editor program is a system software utility that allows the user to create and edit files. During the editing process, no special characters are added. On account of this, the editor utility is used to create the source code.

There are two kinds of editors – line editors and screen editors. Line editor edits files line by line. Screen editor helps to load the file and edit by moving the cursor movement keys. Nowadays, users use only screen editors. Notepad utility in Windows, vi editor in UNIX, Edit utility in MS-DOS are typical examples of screen editors.

Utility Programs

Utility programs are those programs which are frequently used by users during the operation of the computer. These include disk formatting, disk copying, file find programs, file compare utility, sort programs etc. Today such utility programs come bundled along with the OS. Weber [9] describes major categories of utility software as:

1. Utility software to facilitate assessing security and integrity
2. Utility software to facilitate system understanding
3. Utility software to facilitate assessing data quality
4. Utility software to facilitate assessing program quality
5. Utility software to facilitate program development
6. Utility software to facilitate assessing operational efficiency

Categories of Systems

Application systems can be classified into the following groups:

1. Batch processing systems
2. On-line systems
3. Real-Time Systems

In the batch processing system, transactions are collected over a period of time and processed in one stroke. During execution of the task there is very little or no interaction or communication between user and the computer system. One typical example for batch processing system is payroll computation.

In an online system, transactions are processed within a reasonable time of their creation and the results are presented to the user. Typical examples for online systems are in banking, inventory control and financial accounting.

There is only a subtle difference between online and real-time systems. All real-time systems are online while the vice-versa is not true. In the case of a real-time system, as an event occurs, it is processed immediately, output is shown to the user and the system takes corrective steps, if needed. Typical examples of real-time systems include flight control systems, industrial process control, flexible manufacturing applications and cruise control systems in automobiles. Most real-time systems are special purpose and complex systems that require a high degree of fault tolerance and are typically embedded in a larger system.

Information Systems

Any organisation has three main types of information systems that help the three levels of management of strategic, middle-level and first-line management. They are:

Strategic level systems help the top management to address and tackle strategic issues.

Tactical level systems help the middle level of management in monitoring and controlling various functions and activities of the organisation.

Operational level systems are aimed at the first-line managers and help in performing routine activities and track the flow of transactions.

There are categories of systems within these three main types of systems. Table 3 provides details on the same.

Table 3: Types of Information Systems and Characteristic

TYPE OF SYSTEM	CHARACTERISTIC	LEVEL AD-DRESSED	TYPICAL EXAMPLES
Transaction Processing System (TPS)	1. Takes care of routine activities 2. Goals are well-defined and highly structured 3. Computer software available 4. Detailed reports and summaries generated.	First-line management	Payroll, Accounting, Cash management, Purchase order processing, sales-order processing
Office Automation System (OAS)	1. Manages all documents and schedules. 2. Provide support to all levels of management.	All levels	Word processing, e-mail, electronic calendars
Management Information Systems (MIS)	1. Primary goal is to serve the functions of planning, organising and controlling various activities. 2. Information requirements are known and stable 3. Orientation is more towards exceptional reporting rather than regular reporting.	Middle level	Inventory control, Budgeting
Decision Support Systems (DSS)	1. Addresses semi-structured problems 2. Tuned and adapted to the decision maker 3. Uses databases, mathematical models and performs sophisticated analysis	Middle level	Cost-analysis, Production Scheduling
Executive Support Systems (ESS)	1. Focus is on unstructured problems. 2. Has to deal with problems that deal with uncertainty. 3. Provide a generalized computing environment.	Strategic Level	Acquisition, mergers and take-overs,

Client/Server Architectures

If one looks at the path by which computer architectures have evolved, one would come across the following:

Mainframes / Machines with Time-shared concept: With mainframe/ machines with time-shared concept, the entire architecture is dependent on the central computer. Users interact with the host through a terminal that simply captures keystrokes and sends that information to the

Module 1, Chapter 2

host. Only the host does all processing. Mainframe machines of today use dumb terminals as well as PCs. The main limitation of mainframe includes high cost (for both installation and maintenance), limited scalability and poor support for graphical user interfaces.

Network based architectures / File sharing architecture: In the early LAN architectures, a central server held all files and the processing took place in the nodes in the user end. Whenever there is a processing requirements, nodes will request the server for relevant data and these data will traverse through the network and the processed data would again traverse back to the server. If the shared usage is low, update contention is low, and the volume of data to be transferred is low, file server based systems work satisfactorily. However, in cases of large volume data processing, load on the system and the network increased tremendously which led to the development of client/server architecture.

Client/server architecture. In this architecture, there exists a server and a client. The file server in the Network based architecture was replaced by a database server. To query the database server, database management system (DBMS) software is used.

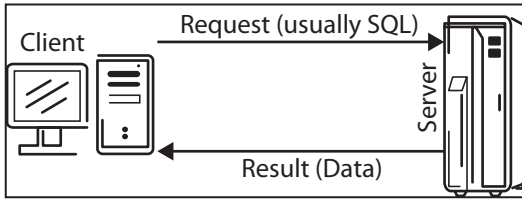
The basic components of a client/server system are :

1. Client
2. Server
3. A robust and good communication system
4. A GUI based operating system
5. Open-database Connectivity drivers (ODBC) and Application Programming Interfaces (APIs)

How a Client Server System Works:

1. The user submits a job to the client.
2. The client processes the job and determines what is to be done. This is the client-side part of the job.
3. The job is then transferred to the server via the communication system.
4. The server, upon receiving the job, performs the requested process. This is the server-side part of the job.
5. The results are passed back to the client via the communication system.
6. The client then performs some tasks on the job to provide the results to the user in the appropriate fashion.

This clearly indicates that the job is shared between the server and the client. On account of this, there is reduced network traffic. **REMOTE PROCEDURE CALLS (RPCs)** or **STRUCTURED QUERY LANGUAGE (SQL)** statements are typically used to communicate between the client and server. Figure 3 shows the working of a client-server system.

Figure 3: Working of a Client Server System

Client Server architectures are broadly classified into Two –Tier architecture and N-Tier architecture.

Two tier architecture. In a two tier client/server architecture, the user interface (GUI) is in the user's machine and the database management services are usually in the server.

The main disadvantage of a 2-Tier architecture is that when the number of users exceeds a certain value, there is performance degradation.

Three tier architecture. To overcome the problems of two-tier architecture, three-tier architecture was introduced.

In the three tier architecture, a middle tier (also called as middleware) was added between the client and the server. The middleware provides services such as identification, authentication, authorisation and security.

Introduction to Object-Oriented (O-O) Concepts

O-O concepts and O-O programming are becoming more popular because they are easy to adapt to changing requirements, easy to maintain, robust, allows one to create modules of functionality and once objects are defined, everything will automatically fit into its right place.

In general terms, an object is any real-world entity that can be distinguished from its surroundings. Every object is then described by its properties (attributes) and the methods (functions) that describe the behaviour of the object. To illustrate, consider the object car. The attributes (also called as the data part) of the car, are engine capacity, colour, price, etc. The methods (also called as the logic part) are functions that can be done on the car such as start, accelerate, apply brakes, change gear, etc.

In an O-O environment, a software is a collection of discrete objects that encapsulate data (attributes) as well as functions (methods) to model real-world “objects”.

The following terms describe the various aspects of O-O systems.

Module 1, Chapter 2

Classes

Classes are used to distinguish one type of object from another and is a generic form of an object. They specify the structure of the object, the way the object behaves, and the inheritance parameters. Any object is simply an instance of the class and is uniquely identified by its **NAME** and it defines a **STATE** which is represented by the values of its attributes at a particular time. The state of the object changes according to the methods which are applied to it. One refers to these possible sequences of state changes as the **BEHAVIOUR** of the object. The behaviour of an object is defined by the set of methods which can be applied on it.

Messages

Objects communicate with each other by exchanging messages. They react when they receive messages by applying methods. A message is defined as a request to an object to invoke one of its methods. A message therefore contains:

1. the name of the method and
2. the arguments of the method.

Abstraction

This refers to the property where only the essential and inherent aspects are focussed and other aspects are ignored. By abstraction, the properties of the object are only specified but not fully defined. Each object in the system serves as a model of an abstract “actor” that can perform work, report on and change its state, and “communicate” with other objects in the system, without revealing how these features are implemented.

Encapsulation and information hiding:

Encapsulation is the process by which every object conceals the internal data and procedures and provide an interface in such a way that they reveal as little as possible about the inner workings. The main aspect of encapsulation is that this property ensures that objects cannot change the internal state of other objects; only the object’s own internal methods are allowed to access and change its state. Encapsulation is a way to implement abstraction.

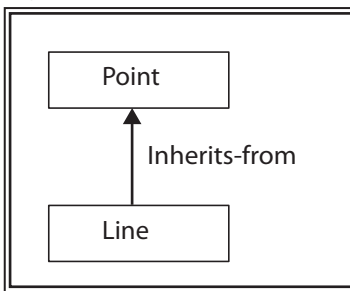
To illustrate the concept of encapsulation, consider again the example of the car. We have cars that run on petrol and cars that run on diesel. While a petrol engine has a spark plug, a diesel engine does not have it. Even though the implementation of the engines are different, a car driver performs very similar operations. i.e. to start the engine, turn on the ignition and press the accelerator for the car to move forward. The details of the implementation of the car engine are insulated from the way they work.

Inheritance

This is a property by which an object acquires its structure and methods from other classes. If class A inherits the properties of a class B, it means that objects of class A have an access to attributes and methods of class B. So class B is called the **SUPERCLASS** of class A. A is called as the **SUBCLASS** of class B. Superclasses are also called **PARENT CLASSES** and subclasses are also referred to as **CHILD CLASSES** or **DERIVED CLASSES**. Inheritance is generally understood from an inheritance graph.

To illustrate this, let's consider a small example from geometry. A line is a sequence of points. Then, a line inherits the characteristics of a point. This is depicted in figure 4.

Figure 4 An inheritance Graph



Inheritance also allows the property of reusability. The methods defined for the superclass can be directly used by the subclass.

Multiple inheritance: Multiple inheritance means that one subclass can have more than one superclass. This enables the subclass to inherit properties of more than one superclass and to “merge” their properties.

Polymorphism

By polymorphism, we mean that objects can take on or assume many different forms. It also means that the same operation may behave differently on different classes. Polymorphism allows one to write generic, reusable code easily.

Using these concepts, the process of O-O systems development consists of the following steps:

1. Perform the O-O analysis. In this step, the user's needs and requirements are translated into system requirements.
2. Perform O-O design. Here, a detailed design is created from the analysis.
3. Perform O-O implementation: From the design, a prototype is created and implemented. This implemented system is then tested and documented.

More details on O-O concepts and O-O system development can be had from Bahrami [1] and Rumbaugh [6].

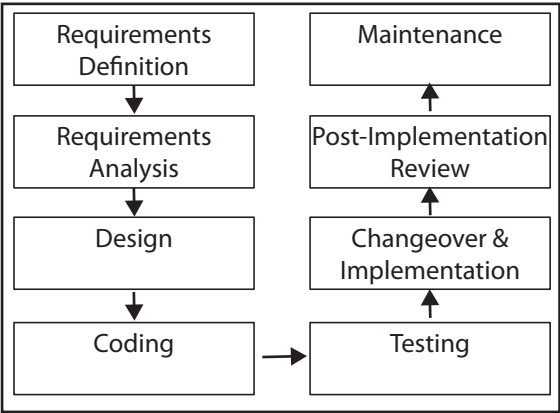
Stages in Software Development

Software development is a complex process which consists of the following stages:

- 1. Requirements definition
- 2. Requirements analysis
- 3. Design
- 4. Coding
- 5. Testing
- 6. Changeover and implementation
- 7. Post-implementation review
- 8. Maintenance

All these stages are depicted in figure 5.

Figure 5: Stages in the software development process



The various functions of each of these stages are described in table 4.

Table 4: Stages in SDLC and their brief description

STAGES	DESCRIPTION
Requirements definition	Requirements definition is the process by which the needs of the customer are translated into a clear, detailed specification of what the system must do.

STAGES	DESCRIPTION
Requirements analysis	In this stage, the development team analyzes the requirements and specifications document for completeness and feasibility. The development team uses structured or object-oriented analysis and resolves ambiguities and discrepancies. Various analyses such as cost-benefit, obsolescence and ROI are done in this stage.
Design	During this phase, the software architecture that meets the system specifications is initially designed. All internal and external interfaces are defined to the subsystem level, and the designs of high-level functions/objects are specified. The following are the output of this stage: 1. Functional or object-oriented design diagrams 2. Descriptions of all user input, system output and input/output files 3. Operational procedures 4. Functional and procedural descriptions of each unit 5. Descriptions of all internal interfaces among units 6. Controls that are to be in place
Coding	During this phase, the developers convert the design specifications of the design stage into a high level program code. The source code is then compiled and documented. For the purpose of coding, specific tools such as source code generator and CASE tools are available.
Testing	This phase focus on testing the software that has been developed. Various types of testing that are carried out on the software include overall specification test, Lines-of-Code (LoC) testing, module testing, interface testing, integration testing, system testing, stress/volume testing, recovery testing, security testing, regression testing, and user acceptance testing.
Changeover and implementation	This is the phase where the old system is replaced by the new system. Various strategies for changeover include direct changeover, parallel changeover, phased changeover and pilot changeover.
Post-implementation review	In post-implementation review, it is verified that the new system that has been developed fulfils the requirements for which it was built. It is also verified whether appropriate controls are in place.
Maintenance	During this phase, the new system is run as a production system. Various types of maintenance such as corrective, adaptive, preventive and perfective are also carried out according to the needs of the user.

The Selection Criteria for Software

1. When purchasing software, it is recommended that companies offering 30 day preview of software be used whenever and wherever possible so that one can use the same and evaluate whether the software will be suitable.
2. Compatibility of the software with the existing and proposed hardware is important.
3. Ensure that the vendor is a reliable one.
4. The software that is being procured must be compatible with other programs that are being used.
5. The installation and operating procedures of the software must be simple
6. The software must be easy to use.

A series of acquisition steps follow the finalization of software and hardware criteria. The acquisition steps are very similar to that of any capital equipment procurement. The ITT should be sent to vendors and after bids are received, they need to be analyzed under the two major headings of technical and commercial. After analysis, successful bidders are called for negotiations. During negotiations, all aspects including cost, delivery and installation timeframe, maintenance issues, training issues, assistance in changeover, upgrade issues are to be discussed and then a final choice should be arrived at. All contract terms including right to audit clauses have to be finalized and then a final formal report has to be prepared. The report has to specify the reasons for arriving at a particular decision justifying the selection based on benefits and cost.

Summary

In this chapter, we began with describing the software architecture. A brief introduction on systems and application software was presented. Typical examples of various systems software and their functions were elucidated. A detailed description on the functions of operating system was also presented. This was followed by the generations of languages. The basic concepts of abstraction, encapsulation, inheritance and polymorphism with regard to Object oriented systems were discussed. Important types of information systems such as TPS, OAS, MIS, DSS, and ESS were also discussed. Finally, the chapter concluded with a brief discussion on the various stages of software development with emphasis on change control procedures.

References

1. Bahrami A, Object Oriented Systems Development - An unified approach, McGraw Hill International edition, New York, 1999.

Module 1, Chapter 2

2. Beck, Leland L, Systems Software, Pearson Education India, New Delhi, 2002.
3. Berson A and Anderson, Sybase and Client-Server Computing, McGraw Hill International edition, New York, 1999.
4. Laudon and Laudon, Management Information Systems, Prentice Hall of India, New Delhi, 1999.
5. Pressman R, Software Engineering, a Practitioner's approach, Tata McGraw Hill, New Delhi, 1999.
6. Rumbaugh J, et al, Object Oriented Modeling and Design, Prentice Hall of India, New Delhi, 2002.
7. Sommerville I, Software Engineering, Addison Wesley Publishing.
8. Stallings W, Operating Systems, 4th edition, Prentice Hall of India, New Delhi, 2003.
9. Weber R, Information Systems Control and Audit, Pearson Education India, New Delhi, 2002.



3 Database Management Systems

✂ Learning Goals ✂

The topics covered in this chapter are:

1. Introduction
2. What is a Database and Database Management Systems (DBMS)
3. DBMS architecture
4. DBMS models
5. Database Languages
6. SQL
7. Roles and duties of a Database Administrator (DBA) and Data Administrator (DA)
8. Database Failures and Recovery Procedures

After reading this chapter, one must be able to understand the importance of databases and DBMS software.

Introduction

Survival of organisations depends on its ability to quickly find the right information at the right time so that appropriate decisions can be taken. The amount of information an organisation handles is exploding day-by-day and unless they use a Database Management System Software, managing the data becomes virtually impossible. It is in this context, the contents of this chapter are relevant.

What is a Database and Database Management Systems (DBMS)

Prior to databases, organisations adopted file concept for storing data. Here, data is stored in flat-files and computer programs were written to access this data. The main drawbacks of this method are:

1. Very high degree of data redundancy: Since data is required by more than one application, data is recorded in multiple files, thus causing data redundancy. High data redundancy leads to multiple updating, problems of maintaining integrity and so forth. Moreover, data redundancy may result in inconsistency - one might update data in one file forgetting to update the same data stored in another file.
2. In the flat file method, data sharing is very limited.
3. For every new query, a new application has to be developed.
4. High degree of dependency between data and programs: Data in flat files are accessed using application programs. If any change in the

Module 1, Chapter 3

data structure or format is made in the data file, a corresponding change has to be done in the application program and vice versa.

These reasons led to the development of databases and DBMS software.

A database is defined as a centralised repository of all the inter-related information of an organisation stored with the objectives of:

1. **Permitting data sharing:** Being centralised in nature, data in a database is allowed to be shared among users and applications.
2. **Minimising data redundancy:** Since only one copy of the data is available which is shared among the users, redundancy is minimal.
3. **Enforcing standards:** Overall standards specified by the company's policies can be enforced.
4. **Providing higher degree of data security and integrity:** Since data is available at a single centralised location, high degree of data security and integrity can be achieved.
5. **Achieving program/data independence:** In contrast to conventional data files, degree of dependency between program and data is very low i.e. application programs are insulated from changes in the way the data is structured and stored. In other words, application programs can be altered without changes in the structure of the data and the database can be changed without the need for reprogramming.
6. **Faster application program development.**

A Database Management System (DBMS) is software that manages a database and provides facilities for database creation, populating data, data storage, data retrieval and data access control.

DBMS Architecture

Figure 1 below shows the architecture of a DBMS. The DBMS software has three main layers of External schema, Conceptual Schema and Internal schema. The functions of various layers are described below.

External Schema

External schema provides the necessary interface for the users to perform various activities on the database and provides the user's view of the database. It is more user-friendly and more focused on users who use the system and the design of the external schema is guided by end user requirements.

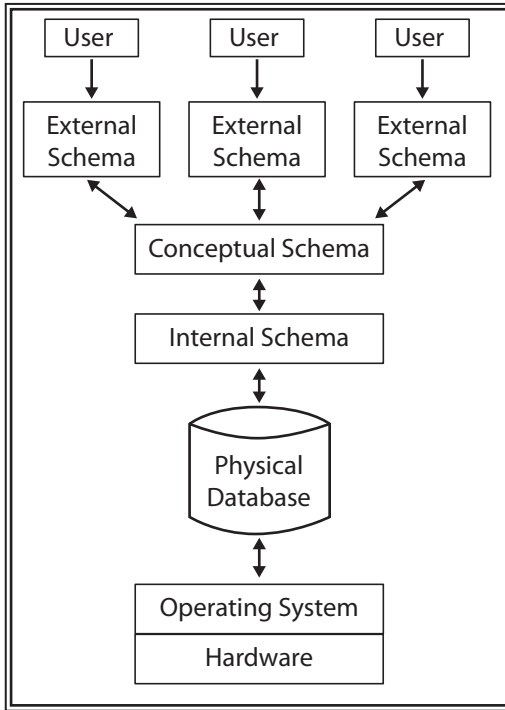
Conceptual schema

The conceptual schema describes the data that is stored in the database in terms of the data model of the DBMS. It provides an abstract way of representing the database.

Internal Schema

The internal schema describes the way the data is physically stored in the database. It specifies the file organisations that are used and the methods by which data is retrieved from the database.

Figure 1: Architecture of a Database Management System



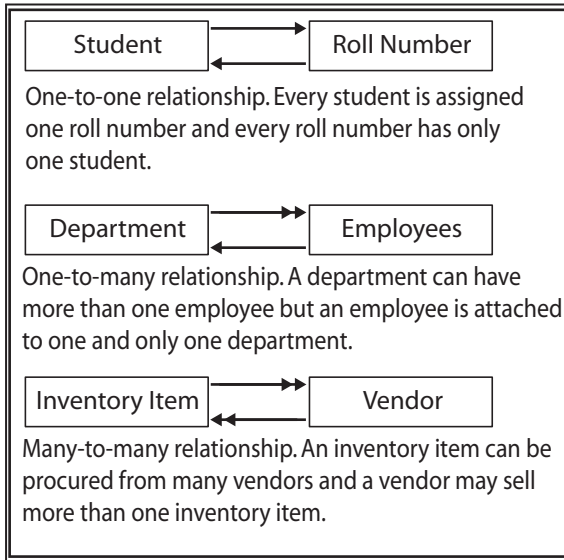
DBMS models

Before a database can be designed and implemented, the decision makers have to develop a conceptual model that contains the entities and their relationships. This conceptual model has to be mapped to the logical model and further mapped into the physical model. First we shall define what an entity is and the relationships that can exist between them.

An entity is an object in the real world that is distinguishable from other objects. An entity is described using a set of attributes. Entities are connected to one another via certain relationships. In other words, a relationship is an association among two or more entities.

Various types of relationship that can be envisaged are “one-to-one”, “one-to-many” and “many-to-many”. Figure 2 shows the various types of relationships with examples.

Figure 2: Illustration showing the types of relationships



Based on the type of relationship that exists between entities, three types of data models can be defined. The main difference between these three models is the way they represent the relationships among entities. The three data models are:

1. Hierarchical model
2. Network or Plex model
3. Relational model

Hierarchical Model

The basis for this model is the hierarchical tree structure. A hierarchical tree structure is made up of nodes and branches. A node is a collection of data attributes describing an entity. The following are the characteristics of a tree structure.

1. There exists a highest node in the tree called the root node.
2. Every node in the tree has one and only parent.
3. A parent node can have any number of children.
4. No loops or cycles are permitted.
5. Every node has to be accessed only through its parent node.

A hierarchical model supports only “one-to-one” and “one-to-many” relationship. The main problem faced in hierarchical model is that unduly complex operations are involved in insertion of nodes in a tree. Moreover the problem of triggered deletion also exists. When a node is deleted from a tree, its children get deleted automatically. This cascading operation is termed as triggered deletion.

IBM's Information Management System is the only DBMS that is implemented using hierarchical model.

Network or Plex Model

The specification for network model was provided by CODASYL DBTG (Conference On Data Systems Language - Database Task Group) report. This model has three basic components: record type, data items and links. This model, unlike hierarchical model supports “many-to-many” relationship. The main disadvantage of this model is its complexity. Also, when the database is reorganised, there is every possibility that data independence might be lost.

Relational Model

See following section.

Relational Model

This is the most common model that is adopted today in majority of commercial DBMS packages. This model has a very strong mathematical backing through relational algebra and relational calculus. Relational Algebra is a low-level, operator-oriented language. Creating a query in Relational Algebra involves combining relational operators using algebraic notation. Relational Calculus is a high-level, declarative language. Creating a query in Relational Calculus involves describing what results are desired.

Dr. E. F. Codd, who has proposed the relational model, has provided twelve rules for the same. The basic characteristics of a relational model are:

1. Data is represented in a two-dimensional table. (i.e. as rows and columns)
2. No two rows can be identical or duplicate rows are not allowed.
3. Ordering of rows is insignificant.
4. Ordering of columns is also insignificant.
5. All data items stored are atomic in nature, that is, they cannot be split further without loss of information.
6. All entries in a column belong to the same category.
7. In majority of the tables, there exists a column called the key column whose value is unique and cannot be null.

Because of the simplicity of usage, relational model has found wide acceptance among the database developers and users community.

Relational data integrity

In order to maintain integrity (accuracy) of data in the database, relational model specifies several types of integrity constraints. The major types of integrity constraints are:

1. **Domain constraint:** This means that all the values that appear in a column of a table must be from the same domain.
2. **Entity integrity:** This rule is to ensure and assure that the data values for the primary key are all valid and not null.
3. **Referential Integrity:** In a relational data model, associations between tables are defined using foreign keys. The referential integrity rule states that if there is a foreign key in one table, either the foreign key must match the primary key of the other table or else the foreign key value must be null.
4. **Operational Constraints:** These constraints are enforced on the database by the business rules or by the environment where the table operates. The database must not violate these constraints.

Data Dictionary

Data Dictionary is a tool that enables one to control and manage the information in a database. It is actually a documentation of the database that provides detailed description of every data that is in the database. It acts as a catalogue providing information on the following:

1. The way data is defined
2. Types of data that is present
3. Relationship among various data entities and their representation formats
4. Keys for the database
5. People who are accessing the data and access rules for every user

A data dictionary also generates various reports on:

1. Various data elements, their characteristics, entities and their relationships.
2. Frequency of usage of data
3. Responsibilities of various users
4. Access control information

A data dictionary is used as an effective tool by the administration in the design, implementation, and operation phases of the database.

Database Languages

A DBMS provides a comprehensive set of facilities, in order to perform the following actions:

1. creating, modifying, deleting database objects,
2. inserting, updating and deleting data in the database,
3. performing the process of querying the database

4. controlling access to the database
5. providing facilities for data integrity and consistency

These facilities are grouped under database languages. There are three important classifications of database languages. They are Data Definition/Description Language (DDL), Data Manipulation Language (DML) and Data Control Language (DCL) .

DDL statements are used to define a database, build and modify the structure of tables and other objects in the database. They are also used for establishing constraints. Data in the database is not touched by the DDL statement. When one executes a DDL statement, it takes effect immediately.

DML statements are used to maintain and query a database.

DCL Statements control a database, including administering privileges and committing data.

Structured Query Language (SQL)

SQL (Structured Query Language) is a database sub-language used for various actions involving relational databases. It was developed by IBM Research Lab in the mid 70's and standardized by ANSI in 1986.

Tables 1,2, and 3 provide a partial list of DDL, DCL and DML commands. For the exact syntax of the command and its usage, one is asked to refer to the documentation of the DBMS package.

Table 1: Partial list of DDL commands.

SQL COMMAND	PURPOSE
ALTER TABLE	Adding a field to the records in a table
ALTER TABLE ADD CONSTRAINT	Adds a constraint to an existing table
ANALYZE	Gathers performance statistics for database objects
CREATE DATABASE	Create a database
CREATE TABLE	Create a table in the database
CREATE VIEW	Create views
CREATE INDEX	Creates an index
DROP VIEW	Delete a view from the database
GRANT	Grants privileges to users
REVOKE	Removes privileges to users

Module 1, Chapter 3

Table 2: Partial list of DCL commands.

SQL COMMAND	PURPOSE
COMMIT	Commit all changes for the current transaction
ROLLBACK	Roll back all changes for the current transaction

Table 3: Partial list of DML commands

SQL COMMAND	PURPOSE
INSERT	Add rows to tables
UPDATE	Modify columns in table rows
DELETE	Removes rows from tables
SELECT	Queries data from tables in the database. In the SELECT command, comparison operators that can be used are: =, !=, <>, <, >, <=, >= and LIKE. One can also use Boolean operators to specify more than one condition (OR, AND, NOT, BETWEEN, IN). With 'BETWEEN' one can give a minimum and maximum value to the condition, with 'IN' one can give a list of values. Moreover, there are a lot of built-in functions. Some of them are given below. All these are used in conjunction with the SELECT command.
Built-in Function: SUBSTRING	Extracts a substring from a string
Built-in Function : UPPER	Converts any lowercase characters in a string to uppercase.
Built-in Function : LOWER	Converts any uppercase characters in a string to lowercase.
Built-in Function : TRIM	Trims leading, trailing or both characters from a string
Built-in Function : POSITION	Searches a string, for a match on a substring
Built-in Function : CHAR_LENGTH	Returns the integer number of characters in the string
Built-in Function : OCTET_LENGTH	Returns the integer number of octets (8-bit bytes) needed to represent the string
Built-in Function : CURRENT_USER	same as USER
Built-in Function : SESSION_USER	Returns a string with the current SQL session authorization identifier.

SQL COMMAND	PURPOSE
Built-in Function : SYSTEM_USER	Returns a string with the current operating system user
Built-in Function : CURRENT_DATE	Returns a Date value for the current system date.
Built-in Function : CURRENT_TIME	Returns a Time value for the current system time.
Built-in Function : AVG	Returns the arithmetic average of the fields.
Built-in Function : COUNT	Returns the number of records that match the condition.
Built-in Function : MAX	Returns the maximum value
Built-in Function : MIN	Returns the minimum value
Built-in Function : SUM	Returns the summation value
Arithmetic Built-in Functions	SQL supports various arithmetic functions. Some of them are ACOS, ASIN, ATAN, ATAN2, COS, COT, SIN, TAN, DEGREES, RADIANS, CEILING, FLOOR, EXP, LOG, LOG10, PI(), POWER, ABS, RAND, ROUND, SIGN, SQRT.

Database access methodology

The process of accessing the database involves three stages:

Stage 1: **Identification Stage:** Here the user identifies who they are to the system. Normally this is done using log-on ids.

Stage 2: **Authentication Stage:** After identification, the users have to authenticate themselves. Normally, passwords are the most common method for authentication. However, today apart from password, other techniques such as biometric identification techniques, Kerberos (trusted 3rd party authentication) have also become more widespread.

Stage3: **Authorisation Stage:** In this stage, what operations can a user perform, on which objects and where these operations can be performed are decided. For this the system maintains an authorisation matrix which helps this process. The authorisation matrix contains information such as subject, object, action and constraint.

Roles and duties of a database administrator

The database administrator (DBA) is responsible for all the technical operations in a database in an organisation.

The major responsibilities of a DBA can be classified under various headings:

1. Management Tasks
 - a. Perform the process of liaising with management.
 - b. Perform the process of liaising with database users for their needs.
 - c. Perform the process of liaising with database vendors
 - d. Perform the process of liaising with the Data Administrator (DA)
 - e. Acquire latest information on database technologies and tools
 - f. Prepare the project status report on the usage of databases
 - g. Prepare the staff requirements
 - h. Prepare budgets
2. Security tasks
 - a. Monitoring and maintaining security of databases.
 - b. Granting access rights and revoking them to users.
3. Technical Tasks
 - a. Monitoring the databases, perform database tuning and optimising database performance.
 - b. Maintaining availability (24 X 365) and ensuring integrity of databases.
 - c. Installing any patch software, if necessary.
 - d. Managing database backups and restorations.
 - e. Guiding application programmers in their work.
 - f. Perform the process of capacity planning.
 - g. Perform the process of normalisation, denormalisation, indexing, and defining views.
 - h. Procedures for purging and archiving data
4. General Tasks
 - a. Providing education and training suggestions
 - b. Ensuring that there is a congenial environment for the people to work.

As mentioned in the management tasks, a DBA has to liaise with the Data Administrator (DA). A DA is a person who identifies the data requirements of the business users by creating an enterprise data model. He identifies the data owners and sets standards for control and usage of data. Weber [5] compares the major duties and responsibilities of DA and DBA which is discussed elsewhere in this material.

Database Failures and Recovery Procedures

Database failures can be catastrophic for the working of the organisation. In this section, we provide only the preliminary aspects for database recovery. Detailed explanation on the same is provided at a latter section in this material.

The possible reasons for database failures include:

1. Failure of the hardware
2. Failure of the operating system
3. Faulty operations (Human errors)
4. Failure of the DBMS
5. Failure of a program
6. Failure of a statement in the program

It is absolutely essential that suitable and appropriate recovery procedures be established in the organisation. Weber [5] identifies the main methods for database recovery as:

1. Grandfather/Father/Son strategy
2. Dual recording / Mirroring strategy
3. Dumping
4. Residual Dumping
5. Logging
6. Differential files

Grandfather/Father/Son strategy

This is a conventional strategy adopted even in legacy systems. Here, at a point of time, three backed up copies of the data are available. What is backed up today is called as the “Son” copy, one that was backed up yesterday is the “Father” and the one of day-before-yesterday is “Grandfather”. Should a failure of the database occur, the data is retrieved by running the updation program taking the “Father” copy and the transaction file.

Dual Recording/Mirroring

This method is used in critical applications. In this strategy, two separate copies of the database are maintained at two geographically different locations. One copy of the database is termed as the primary copy and the other one the secondary copy. Both these copies are simultaneously updated by the updation program. Should the primary copy fail, data is recovered from the secondary copy. The main advantage is that the time for recovery is minimal but the cost is high. Moreover, this technique offers less protection against procedural error when both the primary and secondary copies will be updated with erroneous data.

Dumping

In this process, the entire contents of the database or portions of the database are copied onto a back-up medium. If the database to be dumped is large in size, then this process consumes substantial amount of time and resources.

Residual Dumping

As mentioned earlier, the main problem in the case of dumping is that the process consumes substantial amount of resources and during the time of dumping, the database remains unavailable. To overcome this problem, the idea of residual dumping was proposed and implemented.

In residual dumping method, a log of the records that have not changed since the last dump is taken. This method is used in conjunction with the logging strategy.

Logging

In this method, the focus is on recording a transaction that changes a database or an image of the record changed by an updation program.

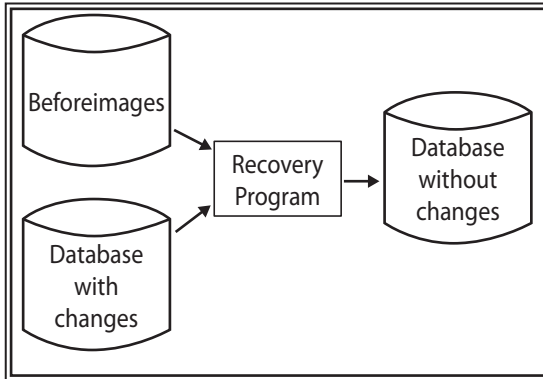
Weber [5] mentions the three logging strategies as:

1. Logging input transactions
2. Logging beforeimages
3. Logging afterimages

In logging input transaction method, the entire updation process is repeated from the point of last dump to the point of failure. The recovery program reads the log file and updates the database in the same way as the application program.

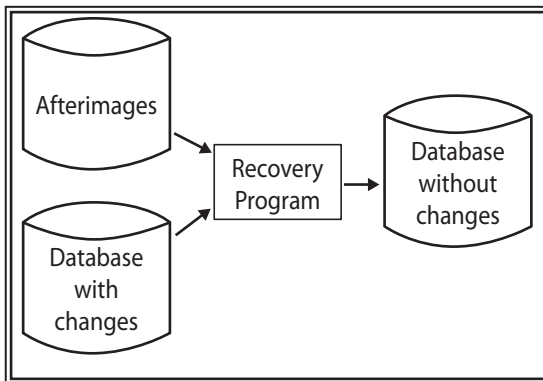
The term beforeimages refers to the copy of the database before modification. In this method of logging beforeimages, a copy of the database before it is updated is logged and so are the transactions. When a failure occurs, the recovery procedure reads the beforeimages and the database with changes to arrive at the database without changes. This process is termed as roll-backward. Figure 4 shows this process.

Figure 4: Database recovery using Beforeimages (Rollbackward Process)



The term afterimages refers to the copy of the database after modification. In this method of logging afterimages, a copy of the database after it is updated is logged and so are the transactions. When a failure occurs, the recovery procedure reads the afterimages and the database with changes to arrive at the database without changes. This process is termed as roll-forward. Figure 5 shows this process.

Figure 5: Database recovery using Afterimages (Rollforward Process)



Differential Files

This is another strategy for database recovery. Here the original database is kept intact, untouched. Records which undergo changes are written into a totally new file called the differential file. As time progresses, when the size of the differential file grows and becomes difficult to manage, the changes are applied to the database.

Summary

This chapter focussed on the preliminaries of databases and DBMS. The need for databases and DBMS software was highlighted. The architecture of a DBMS was also presented. The three important Database models of Hierarchical, Network and Relational were discussed along with their advantages and disadvantages. Concepts on data dictionary, data normalisation techniques were presented. Databases language classification of DDL, DML and DCL in conjunction with a detailed exposition of SQL was presented. The roles and duties of a DBA and database recovery procedures were also discussed.

References

1. Abbey M and Corey M J, Oracle8, A beginners guide, Tata McGraw Hill, New Delhi, 1999.
2. Leon A and Leon M, Database Management Systems, Vikas Publishing, Chennai, 2002
3. Ramakrishnan R, Database Management Systems, McGraw Hill International Edition, New York, 2001.
4. Ullman J, Widom, A first course on database systems, Pearson Education India, New Delhi, 2002.
5. Weber R, Information Systems Control and Audit, Pearson Education India, New Delhi, 2002.
6. <http://www.firstsql.com>



Questions

- Q1. The primary function of the CPU is to take care of :
- A. Input, Output and arithmetic-logic activities
 - B. Control and Output activities
 - C. Control and arithmetic-logic activities
 - D. Input and Control activities
- Q2. Data in a PC is represented by
- A. ASCII Code
 - B. EBCDIC Code
 - C. Gray Code
 - D. Excess - 3 Code
- Q3. Which of the following device is a random access media?
- A. Magnetic Tape
 - B. DAT
 - C. CD-ROM

- D. None of the above
- Q4. When the computer is switched on, the system performs some tasks before loading the operating system. Such ROM chips can be classified as:
- A. Hardware
 - B. Software
 - C. Firmware
 - D. None of the above
- Q5. One feature provided by the OS is to store all the data and program in the auxiliary memory and bring only selective and needed portions into the main memory for processing. This feature is termed as:
- A. Spooling
 - B. Multiplexing
 - C. Caching
 - D. Paging
- Q6. Which of the following is NOT a function of the kernel of the OS?
- A. To determine which processes are to be executed.
 - B. To prepare the access matrix for accessing resources.
 - C. To allocate quantum of main memory for each and every user.
 - D. To overcome the problem of deadlock
- Q7. In its truest sense, which of the following applications is a real time application ?
- A. Missile launching system
 - B. Railway Reservation System
 - C. Banking application
 - D. Financial Accounting system
- Q8. As an IS auditor, what precautionary method would you suggest to the company when old computers that held confidential data are being disposed off:
- A. Dispose it off to reliable people
 - B. Format the hard disk
 - C. Delete all files in the hard disk
 - D. Demagnetize the hard disk
- Q9. Which of the following is NOT addressed in data and capacity management?
- A. Rapid growth of volumes of data
 - B. Rapid growth in the number of computer systems in the organisation
 - C. Effective data backup schemes
 - D. Ensuring 24 X 7 availability

Module 1, Questions

- Q10. Which one of the following is the most essential activity for effective computer capacity planning?
- A. Doing the process of liaison with the management and hardware suppliers
 - B. Talking to security administrator for incorporating security procedures
 - C. To perform the process of Disaster Recovery Planning and Business Continuity Planning
 - D. Determining the workload of applications
- Q11. An Invitation to Tender (ITT) does not address which of the following?
- A. Availability of service personnel
 - B. Application portfolio and transaction volumes
 - C. Budget for the project
 - D. Compatibility of the new systems with the existing ones
- Q12. Which of the following is the best option with regard to an Information Processing Facility (IPF)?
- A. High MTBF and Low MTTR
 - B. Low MTBF and High MTTR
 - C. Low MTBF and Low MTTR
 - D. High MTBF and High MTTR
- Q13. Which of the following is NOT a key concept of object-oriented technology?
- A. Encapsulation
 - B. Cohesion and Coupling
 - C. Polymorphism
 - D. Inheritance
- Q14. Software that translates a program in 2GL to 1GL is:
- A. Compiler
 - B. Interpreter
 - C. Assembler
 - D. Editor
- Q15. If a program is written using mnemonics and op-codes then the program is in
- A. Machine language
 - B. Assembly Level Language
 - C. Procedural Language
 - D. Non-procedural language
- Q16. Which of the following tool would be used when program coding has to be done?
- A. Compiler
 - B. Editor

- C. Loader
 - D. Linker
- Q17. Which of the following is FALSE with respect to Systems Software?
- A. Provides facilities for debugging systems
 - B. Provides facilities to optimally use the resources of the system
 - C. Provides software for cryptographic purpose
 - D. Provides facilities to manage users connected to the system
- Q18. Which of the following is not a job scheduling algorithm?
- A. Round Robin
 - B. Demand Paging
 - C. Shortest Setup time
 - D. Jobs with a Red Tag
- Q19. Which of the following provide complete information about a database?
- A. Database model
 - B. The internal schema of the database
 - C. Data Dictionary
 - D. Database Views
- Q20. Which of the following is NOT considered as a method for data representation in a DBMS?
- A. Hierarchical model
 - B. Indexed Sequential model
 - C. Network model
 - D. Relational model
- Q21. Which of the following statements about a DBMS is INCORRECT?
- A. Data redundancy is minimised
 - B. Applications share data
 - C. Provides the logic to solve a problem in an application
 - D. Provides facilities to access & store data which is accessed by users.
- Q22. The database administrator is NOT responsible for which one of the following functions?
- A. Physical design of a database
 - B. Security of a database
 - C. Coordinate and resolve conflicting needs and desires of users in their diverse application areas
 - D. Logical design of a database
- Q23. SQL is an example for
- A. 1GL
 - B. 2GL
 - C. 3GL
 - D. 4GL

Module 1, Questions

- Q24. The process of database tuning is carried out by
- A. Data Administrator
 - B. Database Administrator
 - C. Application Programmer
 - D. Systems Programmer
- Q25. Which of the following activities is NOT within the scope of a DBA?
- A. Defining the conceptual schema
 - B. Performing the task of database tuning
 - C. Determining the storage capacity for applications
 - D. Granting and revoking rights of users
- Q26. An organisation decides to migrate from conventional file system to a DBMS. Which of the following will increase on account of such migration?
- A. Programming errors
 - B. Data Entry Errors
 - C. Improper file access
 - D. Loss of parity
- Q27. DBMS is a software package used to create, access and maintain a database. The sub-language of a DBMS that defines a database is:
- A. Data Description Language
 - B. Data Manipulation Language
 - C. Data Control Language
 - D. Data Access Language
- Q28. DSS addresses which of the following?
- A. Structured problems
 - B. Semi-Structured problems
 - C. Un-Structured problems
 - D. Problems that focus on exceptional reporting
- Q29. With regard to a DSS, which of the following statements are TRUE:
- i) It deals with semi-structured problems
 - ii) It tackles problems dealing with uncertainty
 - iii) Permits 'What-if' analysis
- A. i & ii
 - B. ii & iii
 - C. i & iii
 - D. i & ii & iii
- Q30. Middleware is implemented by :
- A. Server Monitor
 - B. Transaction Processing Monitor
 - C. CPU utilisation monitor
 - D. Network connectivity monitor

Answers

Question No	1	2	3	4	5	6	7	8	9	10
Answers	C	A	C	C	D	B	A	D	B	D

Question No	11	12	13	14	15	16	17	18	19	20
Answers	C	A	B	C	B	B	C	B	C	B

Question No	21	22	23	24	25	26	27	28	29	30
Answers	C	D	D	B	A	C	A	B	C	B



Module 2: Communication & Networking Technologies

1 Introduction to Networking

✂ Learning Goals ✂

This chapter deals with the fundamentals of networking concepts with an aim towards understanding:

- ▶ Types of networks: Local area networks, Wide area networks
- ▶ Different types of data transmission like simplex, half-duplex, and full-duplex
- ▶ Main components of networks
- ▶ Peer-to-Peer Networks and Client-Server Networks
- ▶ Network Topologies like bus, star, ring, tree, mesh and wireless are discussed along with the advantages and disadvantages of each
- ▶ The OSI Model along with the functioning of all its seven layers.
- ▶ Different Networking Protocols like Ethernet, Fast Ethernet, LocalTalk, Token Ring, FDDI and the application areas for each.

Introduction to Networking

By themselves, computers are powerful tools. When they are connected in a network, they become even more powerful because the resources that each computer provides can be shared with other computers. The purpose of networks is to enable sharing information and resources.

In the simplest sense, networking means connecting computers so that they can share files, printers, applications, and other computer-related resources. The advantages of networking computers together are:

- ▶ Users can save shared files and documents on a file server rather than storing them in their individual computers.
- ▶ Users can share resources like network printer, which costs much less than having a locally attached printer for each user's computer.
- ▶ Users can share applications running on application servers, which enables users to share data and documents, to send messages, and to collaborate.
- ▶ The job of administering and securing a company's computer resources can be concentrated on a few centralized servers.

Networks can also be classified as:

- ▶ Local Area Networks (LAN), which can range from a few desktop workstations in a small office/home office (SOHO) to several thou-

Module 2, Chapter 1

sand workstations and dozens of servers deployed throughout dozens of buildings in a university campus or in an industrial park.

- ▶ Wide Area Networks (WANs), which might be a company's head office linked to a few branch offices or an enterprise spanning several continents with hundreds of offices and subsidiaries.

Because each network is different and utilizes diverse components, it is important to understand the fundamentals of networking and how networking components interact.

In the computer world, the term network describes two or more connected computers that can share resources such as data, a printer, an Internet connection, applications, or a combination of these. In this section, we'll discuss each type of network and describe the situation that is most appropriate for its use.

Local Area Network

By definition, a local area network (LAN) is limited to a specific area, usually an office, and cannot extend beyond the boundaries of a single building. The first LANs were limited to a range (from a central point to the most distant computer) of 185 meters (about 600 feet) and no more than 30 computers. Today's technology allows a larger LAN, but practical administration limitations require dividing it into small, logical areas called workgroups. A workgroup is a collection of individuals (a sales department, for example) who share the same files and databases over the LAN.

Wide Area Network

A WAN is any network that crosses metropolitan, regional, or national boundaries.

WANs differ from LANs in the following ways:

- ▶ WANs cover greater distances.
- ▶ WAN speeds are slower.
- ▶ WANs can be connected on demand or permanently connected; LANs have permanent connections between stations.
- ▶ WANs can use public or private networks; LANs primarily use private networks.

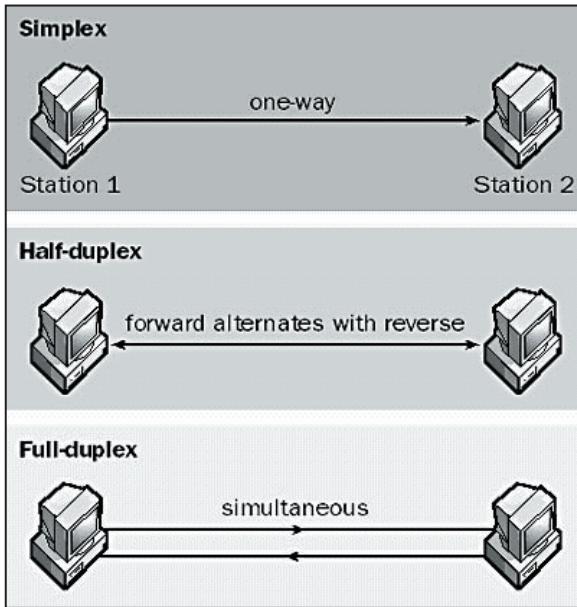
The Internet is actually a specific type of WAN. The Internet is a collection of networks that are interconnected and, therefore, is technically an internetwork. (The term Internet is a contraction of the internetwork).

Simplex, Half-Duplex, and Full-Duplex Communications

All network communications (including LAN and WAN communications) can be categorized as simplex, half-duplex or full-duplex. With simplex, communication can happen in only one direction.

With half-duplex, communications happen in both directions, but in only one direction at a time. When two computers communicate using half-duplex, one computer sends a signal and the other receives; then they switch sending and receiving roles. In a walkie-talkie radio, communication is half-duplex: One person talks, and then the other person talks.

Figure 1: Simplex, Half-Duplex, and Full-Duplex Communications



Full-duplex, on the other hand, allows communication in both directions simultaneously. Both stations can send and receive signals at the same time. Full-duplex communications are similar to a telephone call, in which both people can talk simultaneously.

Methods of Data Transmission

Basically there are two methods of data transmission, viz., asynchronous and synchronous.

Asynchronous Transmission

Also termed as start-stop communications, the asynchronous transmission technique is widely used by computers to provide connectivity to printers, modems, fax machines and the like. In other words, any communication between devices of dissimilar speeds will be an asynchronous one.

The basic characteristics of an asynchronous transmission system are:

1. Sender and receiver have independent transmit and receive clocks
2. Simple interface and inexpensive to implement

Module 2, Chapter 1

3. Limited data rate, typically less than 64 kbps
4. Requires start and stop bits which provides byte timing
5. Increased overhead
6. Parity often used to validate correct reception

Synchronous Transmission

In synchronous transmission, the clock of the receiver is synchronous with the clock of the transmitter. On account of this, higher data transmission rates are possible. There are no start-stop bits. The characteristics of synchronous communication are:

1. Synchronisation between the clocks of the transmitter & receiver,
2. More complex interface
3. Supports high data rates
4. Between computers for specific applications

Workstations and Servers

There are two primary components of a network: workstations and servers. Each one of these items can be found on most networks.

There are two primary components of a network: workstations and servers.

Workstations

In the network environment, the term workstation normally refers to a computer connected to the network that is used by an individual to do work.

It is important to distinguish between workstations and clients. A client is any network entity that can request resources from the network; a workstation is a computer that can request resources. Workstations can be clients, but not all clients are workstations. For example, a printer can request resources from the network, in which case it is a client, but not a workstation.

Servers

In the truest sense, a server does exactly what the name implies: It provides resources to the clients on the network (“serves” them, in other words). Network Servers are typically powerful computers that run the software that controls and maintains the network. This software is known as the network operating system.

Servers are often specialized for a single purpose. Here are some examples of servers that are dedicated to a single task:

- ▶ File Server stores and distributes files.
- ▶ Print Server controls and manages one or more printers for the network.
- ▶ Proxy Server performs a function on behalf of other computers

- Application Server provides storage for network applications.
- Web Server holds and delivers web pages and other web content using the Hypertext Transfer Protocol (HTTP).
- Mail Server hosts and delivers e-mail. It is the electronic equivalent of a post office.
- Fax Server sends and receives faxes for the entire network without the need for paper.
- Remote Access Server hosts modems for inbound requests to connect to the network. Remote access servers provide remote users (working at home or on the road) with a connection to the network.
- Telephony Server functions as a “smart” answering machine for the network. It can also perform call-routing functions.
- Database Server provides storage for the database system
- Notice that each server type contains the name of the service in its name itself.

Regardless of the specific role (or roles) these servers play, they should all have the following in common:

- Hardware and/or software for data integrity (such as backup hardware and software)
- The capability to support a large number of clients
- A server should be located in a physically secure area.

Networks in the Workplace

The purpose of networking is to share resources and information. The way this is accomplished depends on the architecture of the network operating system software. The two most common network types are peer-to-peer and client/server.

Peer-to-Peer Network

In peer-to-peer networks, the connected computers have no centralized authority. From an authority viewpoint, all of these computers are equal. In other words, they are peers. If a user of one computer wants access to a resource on another computer, the security check for access rights is the responsibility of the computer holding the resource.

Each computer in a peer-to-peer network can be both a client that requests resources and a server that provides resources. This is a great arrangement, provided the following conditions are met:

- Each user is responsible for local backup.
- Security considerations are minimal.
- A limited number of computers are involved.

For example, networks that run Windows 95/98 as their network operating system or networks using a workgroup are considered peer-to-peer networks. Peer-to-peer networks present some challenges. Backing up company data becomes a tricky proposition. Also, it can be difficult

Module 2, Chapter 1

to remember where you stored a file. Finally, because security is not centralized, users and passwords must be maintained separately on each machine, Passwords may be different for the same users on different machines.

Client/Server Network

In contrast to a peer-to-peer network, a client/server network uses a network operating system designed to manage the entire network from a centralized location, which is the server. Clients make requests of the server, and the server responds with the information or access to a resource.

Client/server networks have some definite advantages over peer-to-peer networks. For one thing, the network is much more organized. It is easier to find files and resources because they are stored on the server. Also, client/server networks generally have much better security. All usernames and passwords are stored in the server. Finally, client/server networks have better performance and scalability. It is not uncommon to see client/server networks with tens of thousands of workstations.

Network Topologies

A topology is basically a map of a network. The physical topology of a network describes the layout of the cables and workstations and the location of all network components.

The cables or connections in a physical topology are often referred to as network media (or physical media). Choosing how computers will be connected in a company's network is critical. A wrong decision in the physical topology makes the media difficult to correct, because it is costly and disruptive to change an entire installation once it is in place

In this section, we'll look at the most common topologies:

- ▶ Bus
- ▶ Star
- ▶ Ring
- ▶ Tree
- ▶ Mesh
- ▶ Wireless

Bus Topology

In a bus topology, all computers are attached to a single continuous cable that is terminated at both ends, which is the simplest way to create a physical network. Originally, computers were attached to the cable with wiretaps. This did not prove practical, so drop cables are now used to attach computers to the main cable.

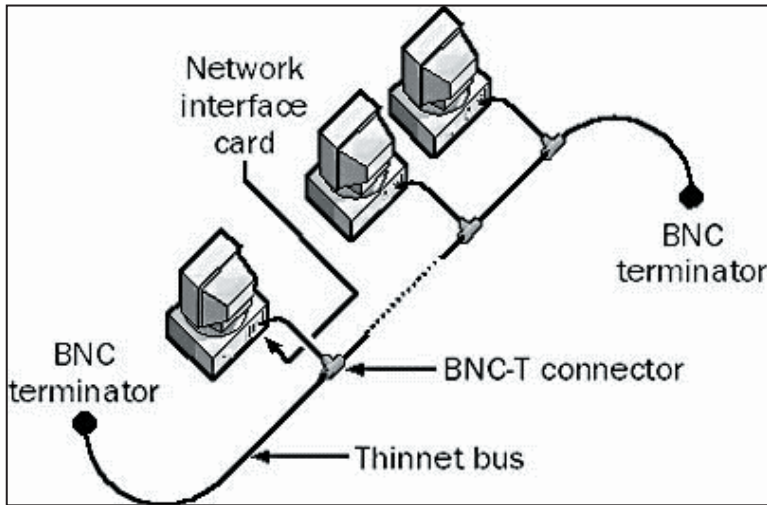
When communicating on a network that uses a bus topology, all computers see the data on the wire. This does not create chaos, though,

because the only computer that actually accepts the data is the one to which it is addressed.

Advantages of Bus topology:

- ▶ Is simple to install
- ▶ Is relatively inexpensive
- ▶ Uses less cable than other topologies

Figure 2: Bus Topology



Disadvantages of Bus topology:

- ▶ Is difficult to move and change
- ▶ Has little fault tolerance (a single fault in the main bus can bring down the entire network)
- ▶ Is difficult to troubleshoot

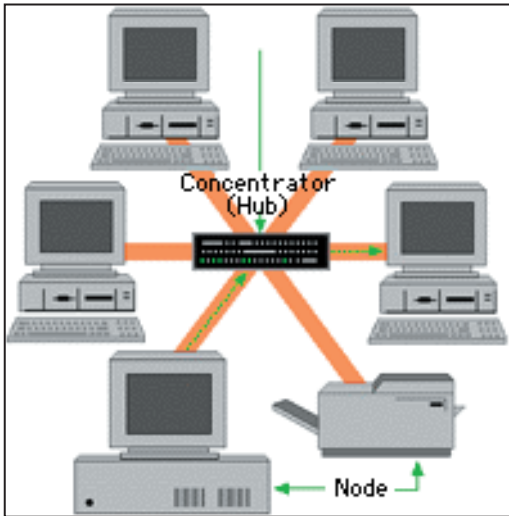
Star Topology

Each computer in a star topology is connected to a central point by a separate cable. The central point is a device known as a hub. Although this setup uses more cable than a bus, a star topology is much more fault-tolerant than a bus topology. This means that if a failure occurs along one of the cables connecting to the hub, only that portion of the network is affected and not the entire network. It also means that you can add new stations just by running a single new cable.

Advantages of Star topology:

- ▶ A failure in a node or cable to the node will not bring down the entire network.
- ▶ It is relatively easy to troubleshoot.
- ▶ New stations can be added easily and quickly.

Figure 3: Star Topology



Disadvantages of Star topology:

- ▶ Total installation cost can be higher because of the larger number of cables, but decreasing price of cables has rendered this disadvantage less serious.
- ▶ It has a single point of failure, the hub.

Ring Topology

In the ring topology, each computer is connected directly to two other computers in the network. Data moves down a one-way path from one computer to another. While adding or removing a computer, the ring needs to be “broken”, hence it is very difficult to re-configure without bringing down the whole network. For this reason, the physical ring topology is seldom used.

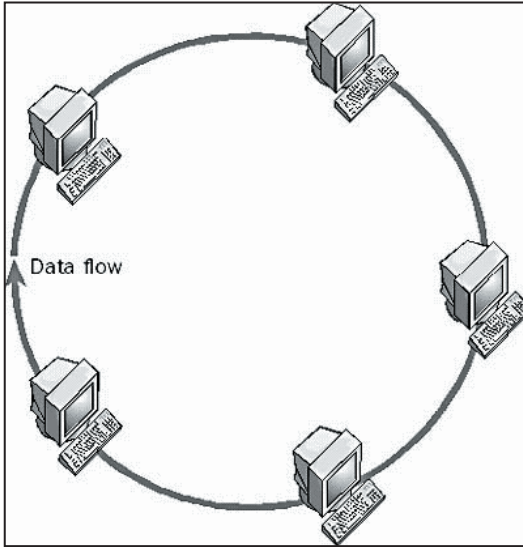
Advantages of Ring topology:

- ▶ The ring topology is relatively easy to troubleshoot. A station will know when a cable fault has occurred because it will stop receiving data from its upstream neighbour.

Disadvantages of Ring topology

- ▶ Expensive, because multiple cables are needed for each workstation.
- ▶ Difficult to re-configure.
- ▶ Not fault tolerant. A single cable fault can bring down the entire network.

Figure 4: Ring Topology



Tree Topology

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network, and enable groups or departments to configure a network to meet their needs.

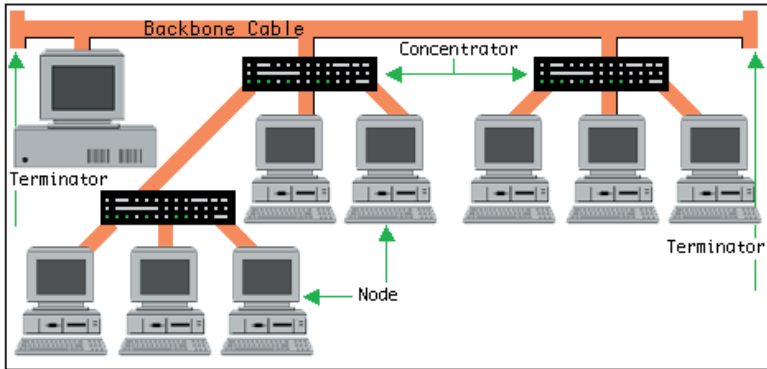
Advantages of a Tree Topology:

- ▶ Point-to-point wiring for individual segments.
- ▶ Supported by several hardware and software vendors.

Disadvantages of a Tree Topology

- ▶ Overall length of each segment is limited by the type of cabling used.
- ▶ If the backbone line breaks, the entire segment goes down.
- ▶ More difficult to configure and wire than other topologies

Figure 5: Tree Topology



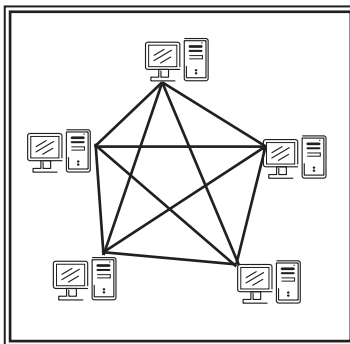
Mesh Topology

A network topology in which additional networking components are used to provide redundant data paths. This topology provides a high level of fault tolerance; if a wire, hub, switch, or other component fails, data can travel along an alternate path. A diagram of a mesh network might resemble a portion of a fishing net. A mesh topology is most often used in large networks in which failure of a connecting device can result in a large portion of the network going down. Mesh networks can be of two kinds:

Full mesh topology: Provides a direct link between each pair of nodes on the network. Full mesh topologies provide the highest level of fault tolerance.

Partial mesh topology: Includes some redundant data paths to provide some level of fault tolerance. This is the more usual implementation in a large internetwork.

Figure 6: Mesh Topology

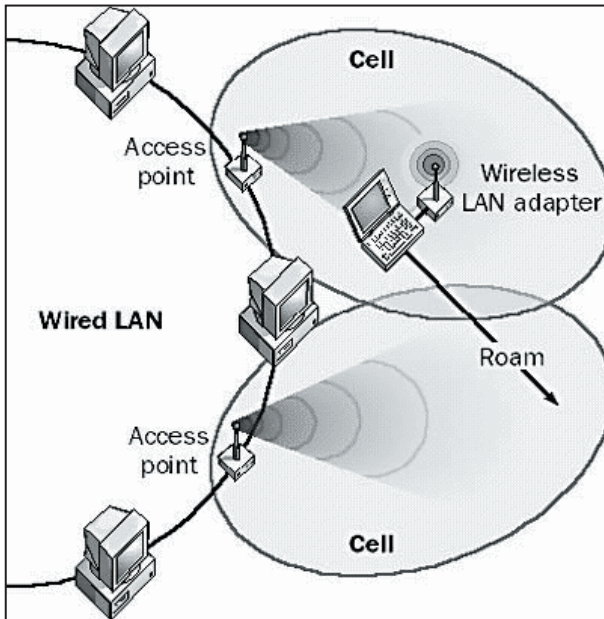


Advantages of Mesh topology:

- ▶ Mesh topology provides a high degree of fault-tolerance and reliability.
- ▶ Disadvantages of Mesh topology:
- ▶ Mesh topology is expensive and complex.
- ▶ Wireless Networking

Wireless networking uses unguided media, as opposed to guided media (copper and fiber-optic), used in traditional wired networks. Wireless networking is typically used for communication with mobile users who roam over large distances, such as sales representatives with laptops.

Figure 7: Wireless Topology



Wireless networks are ideal for work areas in which it is impractical or expensive to run cabling, such as older buildings that are costly to renovate. In this case, two solutions are possible:

- ▶ Create a wireless LAN (WLAN) that uses no cabling between stations.
- ▶ Create a combination of traditional wired local area networks (LANs) and as many wireless stations as needed.

To connect wireless stations to a traditional wired LAN, you need the following components:

- ▶ One or more access points, which are transceivers connected to the wired LAN. They broadcast signals to and receive signals from the wireless stations on the LAN, forwarding signals between the wired network and the wireless stations as needed. The effective reception

Module 2, Chapter 1

range from an access point defines a circular area called a cell. A typical wireless access point device might provide up to 3000 square meters of coverage in open areas (or less when obstacles are present) and support data transmission rates of 1 to 56 Mbps.

- ▶ A WLAN adapter or wireless adapter which turns the computer in which it is installed into a wireless station on the network. A fixed or detachable antenna is generally included and gives the station better transmission and reception. For a small-scale WLAN, the adapter might give a coverage range of about 300 meters in open areas (or less when obstacles are present).

The OSI Model

A wide variety of organizations contribute to internetworking standards by providing forums for discussion, turning informal discussion into formal specifications, and proliferating specifications after they are standardized.

Most standards organizations create formal standards by using specific processes: organizing ideas, discussing the approach, developing draft standards, voting on all or certain aspects of the standards, and then formally releasing the completed standard to the public.

Some of the best-known standards organizations that contribute to internetworking standards include these:

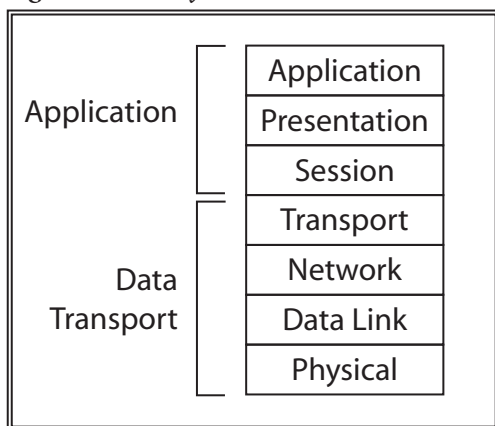
- ▶ International Organization for Standardization (ISO)—ISO is an international standards organization responsible for a wide range of standards, including many that are relevant to networking. Its best-known contribution is the development of the OSI reference model and the OSI protocol suite.
- ▶ American National Standards Institute (ANSI)—ANSI, which is also a member of the ISO, is the coordinating body for voluntary standards groups within the United States. ANSI developed the Fiber Distributed Data Interface (FDDI) and other communications standards.
- ▶ Electronic Industries Association (EIA)—EIA specifies electrical transmission standards, including those used in networking. The EIA developed the widely used EIA/TIA-232 standard (formerly known as RS-232).
- ▶ Institute of Electrical and Electronic Engineers (IEEE)—IEEE is a professional organization that defines networking and other standards. The IEEE developed the widely used LAN standards IEEE 802.3 and IEEE 802.5.
- ▶ International Telecommunication Union Telecommunication Standardization Sector (ITU-T)—Formerly called the Committee for International Telegraph and Telephone (CCITT), ITU-T is now an

international organization that develops communication standards. The ITU-T developed X.25 and other communications standards.

- ▶ Internet Activities Board (IAB)—IAB is a group of internetwork researchers who discuss issues pertinent to the Internet and set Internet policies through decisions and task forces. The IAB designates some Request For Comments (RFC) documents as Internet standards, including Transmission Control Protocol/Internet Protocol (TCP/IP) and the Simple Network Management Protocol (SNMP).
- ▶ The Open Systems Interconnect (OSI) model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for inter-computer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers. The following list details the seven layers of the Open System Interconnection (OSI) reference model:
 - ▼ Layer 7—Application
 - ▼ Layer 6—Presentation
 - ▼ Layer 5—Session
 - ▼ Layer 4—Transport
 - ▼ Layer 3—Network
 - ▼ Layer 2—Data link
 - ▼ ▶ Layer 1—Physical
- ▶ The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers.

The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component.

Figure 8: ISO Layers



The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium.

The OSI reference model is best seen as an idealized model of the logical connections that must occur for network communication to take place. The OSI model is a good starting point for understanding how various protocols within a protocol suite function and interact.

Application Layer

The Application layer, the top layer of the OSI model, does not refer to applications such as word processors, but rather refers to a set of tools that an application can use to accomplish a task, such as a word processor application requesting a file transfer. This layer is responsible for defining how interactions occur between network services (applications) and the network. Services at the Application layer include, but are not limited to, file, print, and messaging services. The Application layer may also support error recovery.

Presentation Layer

The Presentation layer is responsible for formatting data exchange. In this layer, character sets are converted, and data is encrypted. Data may also be compressed in this layer, and this layer usually handles the redirection of data streams.

Session Layer

The Session layer defines how two computers establish, synchronize, maintain, and end a session. Practical functions, such as security authentication, connection ID establishment, data transfer, acknowledgments,

and connection release, take place here. This list is not all-inclusive. Any communications that require milestones or checkpoints are performed here. Once a checkpoint has been crossed, any data not received needs retransmission only from the last good checkpoint. Adjusting checkpoints to account for varied reliability of connections can greatly improve the actual throughput of data transmission.

Transport Layer

The Transport layer is responsible for checking that the data was delivered error-free. It is also used to divide a long message into smaller segments (often called packets) and, in the reverse, take a series of short segments and combine them into one long message. These segments must later be correctly reassembled. This is accomplished through segment sequencing (usually by appending a number to each of the segments).

This layer also handles logical address/name resolution. Additionally, this layer can send an acknowledgment that it received the data packet. This is referred to as an ACK, which is short for acknowledgment. This layer is responsible for the majority of error and flow control in network communications.

Network Layer

The Network layer is responsible for logical addressing and translating logical names into network addresses. A little-known function of the Network layer is prioritizing data. Not all data is of equal importance. Nobody is hurt if an e-mail message is delayed a fraction of a second. Delaying audio or video data a fraction of a second could be disastrous to the message. This prioritization is known as Quality of Service (QoS).

In addition, the Network layer controls congestion, routes data from source to destination. Most routing protocols function at this layer.

Data Link Layer

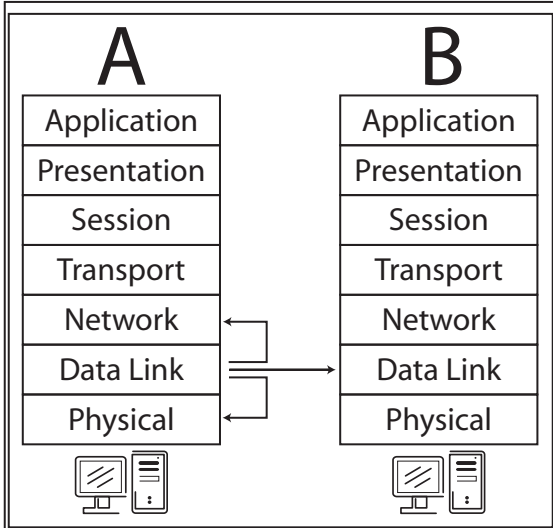
The Data Link layer takes raw data from the Physical layer and gives it a logical structure (called frame). This logic includes information about where the data is meant to go, which computer sent the data, and the overall validity of the bytes sent. In most situations, after a data frame is sent, the Data Link layer then waits for a positive acknowledgement. If one is not received or if the received indicates that the frame is damaged, another frame is sent.

The Data Link layer also controls functions of logical network topologies and physical addressing as well as data transmission synchronization and connection

Physical Layer

The Physical layer is responsible for controlling the functional interface, such as electrical properties (live voltage, signal strength, etc.), pin layout, and connector type.

Figure 4: Communication between and among layers.



Each layer can be thought as being logically connected to the same layer on a different computer on the network. For example, the application layer on one machine communicates with the application layer on another machine. But this communication is logical only; physical communication occurs when packets of data are sent down from the application layer of the transmitting computer, encapsulated with header information by each lower layer, and then put on the wire at the physical layer of the transmitting computer. After traveling along the wire, the packets are picked up by the physical layer of the receiving computer, passed up the seven layers while each layer strips off its associated header information, and then passed to the application layer of the receiving computer, where the receiving application can process the data.

Networking Protocols

Networking protocols consist of a set of rules for sending information over a network. Protocols can include rules concerning any or all of the following functions:

- ▶ Data transmission mechanisms
- ▶ Communication session initiation and termination
- ▶ Addressing and routing
- ▶ Authentication and verification
- ▶ Encryption and compression

- ▶ Error correction

Protocols are usually classified according to the layer they correspond to in the Open Systems Interconnection (OSI) reference model for networking. Types of protocols include the following:

- ▶ Data-link protocols: Govern the framing of data, physical addressing of network nodes, and media access control methods. For local area networks (LANs), these primarily include Ethernet, LocalTalk, Token Ring, and Fiber Distributed Data Interface (FDDI).
- ▶ Network protocols: Handle link services and are responsible for addressing, routing, and error checking. Examples include NetBEUI, Internetwork Packet Exchange (IPX) and Internet Protocol (IP).
- ▶ Transport protocols: Enable the establishment of sessions and ensure reliable flow of data. Examples include NetBEUI, Sequenced Packet Exchange (SPX) and Transmission Control Protocol (TCP).
- ▶ Application layer protocols: Enable applications to access network services. Examples include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), Network News Transfer Protocol (NNTP), X.400, X.500, Server Message Block (SMB), and Network File System (NFS).
- ▶ Some protocols have been developed by specific vendors and then accepted as de facto standards by the industry, while others were initially formulated by independent standards bodies and then accepted and implemented by vendors. The most widely implemented protocols are those relating to TCP/IP and the Internet.

Here we shall be discussing the Data-Link protocols that are mainly concerned with LANs. The most common protocols are:

- ▶ Ethernet
- ▶ Fast Ethernet
- ▶ LocalTalk
- ▶ Token Ring
- ▶ FDDI

Ethernet

The Ethernet protocol is by far the most widely used. Ethernet uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a protocol where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. With this access method, it is normal to have collisions. However, the

Module 2, Chapter 1

delay caused by collisions and re-transmitting is very small and does not normally affect the speed of transmission on the network.

The Ethernet protocol allows for bus, star, or tree topologies. Data can be transmitted over twisted pair, coaxial, or fiber optic cable at a speed of 10 Mbps.

Fast Ethernet

To allow for an increased speed of transmission, the Ethernet protocol has been modified to support speeds of up to 100 Mbps. This is commonly called Fast Ethernet. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fiber optic cable is necessary.

LocalTalk

LocalTalk is a network protocol that was developed by Apple Computer, Inc. for Macintosh computers. The method used by LocalTalk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. LocalTalk adapters and special twisted pair cable can be used to connect a series of computers through the serial port. The Macintosh operating system allows the establishment of a peer-to-peer network without the need for additional software. With the addition of the server version of AppleShare software, a client/server network can be established.

The LocalTalk protocol allows for bus, star, or tree topologies using twisted pair cable. A primary disadvantage of LocalTalk is speed. Its speed of transmission is only 230 Kbps.

Token Ring

The Token Ring protocol is a proprietary system licensed and maintained by IBM since the mid-1980s. The media access method used involves token-passing. In Token Ring, the computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the data is captured by the receiving computer. The Token Ring protocol requires a star-wired ring using twisted pair or fiber optic cable. It can operate at transmission speeds of 4 Mbps or 16 Mbps. Due to the popularity of Ethernet, the use of Token Ring has decreased considerably. IBM has discontinued support for the Token Ring standards.

FDDI

Fiber Distributed Data Interface (FDDI) is a network protocol that is used primarily to interconnect two or more local area networks, often over large distances. The access method used by FDDI also involves token-passing. FDDI uses a dual ring physical topology. Transmission normally occurs on one of the rings; however, if a break occurs, the system keeps moving information by automatically using portions of the second ring to create a new complete ring. A major advantage of FDDI is speed. It operates over fiber optic cable at 100 Mbps.

Protocol Summary

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
Local Talk	Twisted Pair	0.23 Mbps	Bus or Star
Token Ring	Twisted Pair	4 - 16 Mbps	Ring
FDDI	Fiber	100 Mbps	Ring

 Summary

The chapter gave an introduction to network technology. The reader was introduced to different classifications of network. The network components and protocols, important constituents of network were discussed. Through the OSI model, the reader was familiarized with the conceptual foundations of networking. A thorough reading of this chapter will help the reader to get an exposure to advanced concepts in the next chapters and also will equip him with a full ability to understand the networks in real life scenario.



2 Network Hardware and Software

✂ Learning Goals ✂

This chapter deals with the components of networking hardware and software with an aim towards understanding:

- ▶ Different types of network cabling like Unshielded Twisted Pair (UTP) cable, Shielded Twisted Pair (STP) cable, Coaxial cable, Fiber Optic cable, and Wireless communications
- ▶ Different types of networking devices like repeaters, hubs, switches, routers, bridges, Network Interface Cards (NICs) and gateways
- ▶ Different network operating systems like Microsoft Windows NT, Novell NetWare, Unix, Windows 2000 Server Edition and Linux operating system.
- ▶ Issues related to installation and control of Network Applications

Network Cabling

Cable is the medium through which information usually moves from one network device to another. There are several types of cables which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cables and how they relate to other aspects of a network is necessary for the development of a successful network.

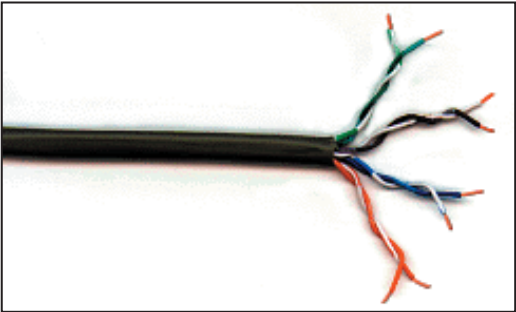
The following sections discuss the types of cables used in networks and other related topics.

- ▶ Unshielded Twisted Pair (UTP) Cable
- ▶ Shielded Twisted Pair (STP) Cable
- ▶ Coaxial Cable
- ▶ Fiber Optic Cable
- ▶ Wireless LANs
- ▶ Installing Cable - Some Guidelines

Unshielded Twisted Pair Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for simple networks.

Figure 1: Unshielded Twisted Pair Cable



The quality of UTP may vary from voice or telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Categories of Unshielded Twisted Pair

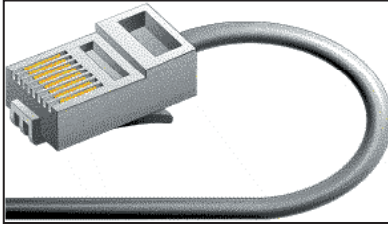
TYPE	USE
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

One difference between the different categories of UTP is the tightness of the twisting of the copper pairs. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. Category 5 cable is highly recommended. Because Category 5 cable will provide more “room to grow” as transmission technologies increase. Both category 3 and category 5 UTP have a maximum segment length of 100 meters. 10BaseT refers to the specifications for unshielded twisted pair cable (category 3, 4, or 5) carrying Ethernet signals.

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is a RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

Figure 2: RJ-45 Connector



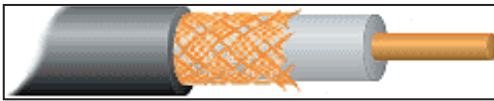
Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electro-magnetic interference (EMI). Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

Figure 3: Coaxial cable



Although coaxial cabling is difficult to install, it is highly resistant to signal interference.

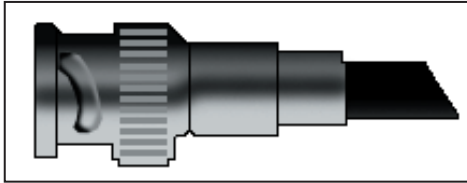
In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are: thick coaxial and thin coaxial.

- ▶ Thin coaxial cable is also referred to as “**THINNET**”. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. Thin coaxial cable is popular in small networks, especially bus networks.
- ▶ Thick coaxial cable is also referred to as “**THICKNET**”. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a lengthy bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayonet-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with the network, always use the BNC connectors that crimp, rather than screw, onto the cable

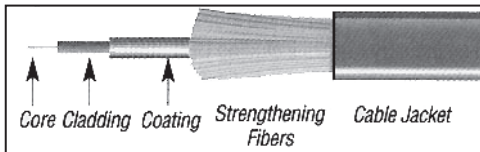
Figure 4: A BNC Connector



Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals, eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Figure 5: Cross section of a fiber optic cable



Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

Facts about fiber optic cables:

- ▶ Outer insulating jacket is made of plastic.
- ▶ Special reinforced plastic fibers helps to strengthen the cable and prevent breakage.
- ▶ A plastic coating is used to cushion the fiber center.
- ▶ Center (core) is made of glass or plastic fibers.

Fiber Optic Connector

The most common connector used with fiber optic cable is an ST connector. It is barrel shaped, similar to a BNC connector. A newer connector, the SC, is becoming more popular. It has a squared face and is easier to connect in a confined space.

Advantages of Fiber Optics

Compared to conventional metal wire (copper wire), optical fibers are:

- ▶ **Less expensive** – Several miles of optical cable can be made cheaper than equivalent lengths of copper wire. This leads to great savings.
- ▶ **Thinner** – Optical fibers can be drawn to smaller diameters than copper wire.
- ▶ **Higher carrying capacity** – Because optical fibers are thinner than copper wires, more fibers can be bundled into a given-diameter cable than copper wires. This allows more phone lines to go over the same cable or more channels to come through the cable into the cable TV box.
- ▶ **Less signal degradation** – The loss of signal in optical fiber is less than in copper wire.
- ▶ **Light signals** – Unlike electrical signals in copper wires, light signals from one fiber do not interfere with those of other fibers in the same cable. This means clearer phone conversations or TV reception.
- ▶ **Low power** – Because signals in optical fibers degrade less, lower-power transmitters can be used instead of the high-voltage electrical transmitters needed for copper wires.
- ▶ **Digital signals** – Optical fibers are ideally suited for carrying digital information, which is especially useful in computer networks.
- ▶ **Non-flammable** – Because no electricity is passed through optical fibers, there is no fire hazard.
- ▶ **Lightweight** – An optical cable weighs less than a comparable copper wire cable. Fiber-optic cables take up less space in the ground.

Cable Summary

SPECIFICATION	CABLE TYPE	MAXIMUM LENGTH
10BaseT	Unshielded Twisted Pair	100 meters
10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Fiber Optic	2000 meters

Wireless LANs

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals or infrared light beams to communicate between the workstations and the file server. Each workstation and file server on a wireless network has some sort of

Module 2, Chapter 2

transceiver/antenna to send and receive the data. Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology or by satellite.

In the broadest sense, wireless networking is composed of all forms of network communication that use electromagnetic waves of any wavelength or frequency, which includes the following portions of the electromagnetic spectrum:

- ▶ **Infrared (IR):** Ranges from frequencies of about 300 GHz to 200 THz and is used primarily in confined areas where line-of-sight communication is possible. IR cannot penetrate buildings or structures, but it can reflect off light-colored surfaces.
- ▶ **Microwave:** Ranges from 2 GHz to 40 GHz and is used for both point-to-point terrestrial communication and satellite communication. Microwave suffers from signal degradation when weather conditions are poor (for example, in fog or rain).
- ▶ **Broadcast radio:** Ranges from 30 MHz to 1 GHz, is less affected by poor atmospheric conditions than microwave, and can travel through most buildings and structures, but suffers from multipath interference over long distances.

Wireless networks are great for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables.

Wireless LANs also have some disadvantages. They are very expensive, provide poor security, and are susceptible to electrical interference from lights and radios.

Wireless networking suffers somewhat from lower data transmission rates (the maximum is currently about 10 Mbps), greater susceptibility to electromagnetic interference (EMI), and greater risk of eavesdropping than transmission over guided media. Users can largely solve the security issue by using secure network protocols, but they should be sure to isolate wireless stations from sources of EMI in the operating frequency range of the network. A microwave oven, for example, can degrade wireless communication that is based on the microwave portion of the electromagnetic spectrum.

Networking Devices

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator.

This section describes the following commonly used networking devices:

- ▶ Network Interface Card (NIC)
- ▶ Repeater
- ▶ Hub/Concentrator
- ▶ Bridge
- ▶ Switch
- ▶ Router
- ▶ Gateway

Network Interface Card

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, with the card fitting into an expansion slot inside the computer.

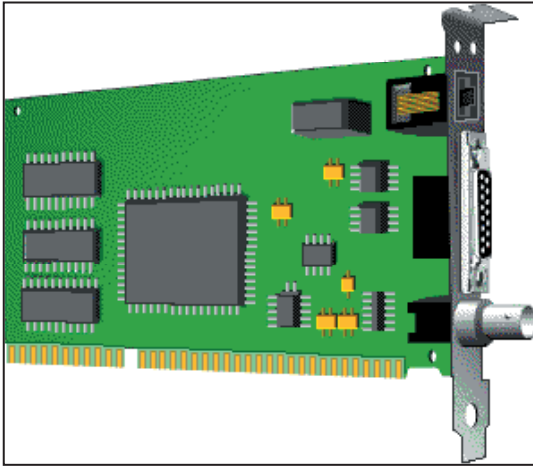
Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation that is being used.

The three most common network interface connections are Ethernet cards, LocalTalk connectors, and Token Ring cards.

Ethernet Cards

Ethernet cards were usually purchased separately from the computer. Today, however, most computers include the network interface on the motherboard itself. Ethernet cards contain connections for either coaxial or twisted pair cables (or both). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection. Some Ethernet cards also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fiber optics cable to an Ethernet card. When this method is used there is always an external transceiver attached to the workstation.

Figure 6: Ethernet card



Token Ring Cards

Token Ring network cards look similar to Ethernet cards. One visible difference is the type of connector on the back end of the card. Token Ring cards generally have a nine pin DIN type connector to attach the card to the network cable.

Repeaters

When a signal travels along a cable, it tends to lose strength. A repeater is a device that boosts a network's signal as it passes through. The repeater does this by electrically amplifying the signal it receives and re-broadcasting it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of the network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a repeater. The repeater regenerates all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 meter limit.

Hubs/Concentrators

Hubs are used in networks that use twisted-pair cabling to connect devices. Hubs can also be joined together to create larger networks. Hubs are simple devices that direct data packets to all devices connected to the hub, regardless of whether the data package is destined for the device. This makes them inefficient devices and can create a performance bottleneck on busy networks.

In their most basic form, a hub does nothing except provide a pathway for the electrical signals to travel along. Such a device is called a passive hub. Far more common nowadays is an active hub, which as well as providing a path for the data signals, regenerates the signal before it forwards it to all of the connected devices. A hub does not perform any processing on the data that it forwards, nor does it perform any error checking.

Hubs come in a variety of shapes and sizes. Small hubs with five or eight connection ports are commonly referred to as workgroup hubs. Others can accommodate larger numbers of devices (normally up to 32). These are referred to as high-density devices. Because hubs don't perform any processing, they do little except enable communication between connected devices. For today's high-demand network applications, something with a little more intelligence is required. That's where switches come in.

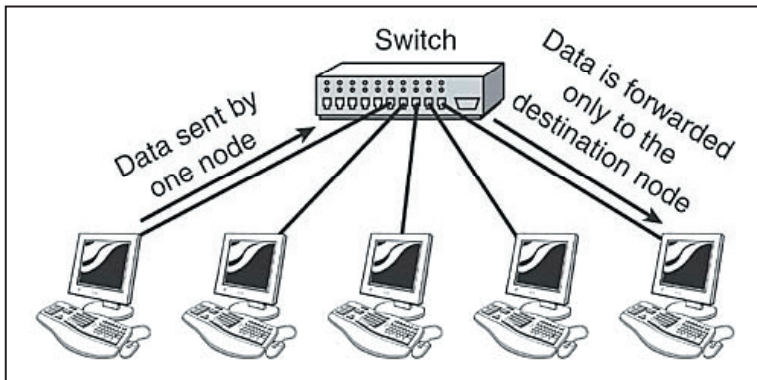
MSAU – Multistation Access Unit

In a Token Ring network, a Multistation Access Unit (MSAU) is used in place of the hub that is used on an Ethernet network. The MSAU performs the token circulation inside the device, giving the network a physical star appearance. Each MSAU has a Ring In (RI) port on the device, which is connected to the Ring Out (RO) port on another MSAU. The last MSAU in the ring is then connected to the first, to complete the ring. Ethernet hubs and switches are much more common than MSAUs.

Switches

Like hubs, switches are the connectivity points of an Ethernet network. Devices connect to switches via twisted-pair cabling, one cable for each device. The difference between hubs and switches is in how the devices deal with the data that they receive. Whereas a hub forwards the data it receives to all of the ports on the device, a switch forwards it only to the port that connects to the destination device. It does this by learning the MAC address of the devices attached to it, and then by matching the destination MAC address in the data it receives.

Figure 7: Switch



By forwarding data only to the connection that should receive it, the switch can improve network performance in two ways. First, by creating a direct path between two devices and controlling their communication, it can greatly reduce the number of collisions on the network. Collisions occur on Ethernet networks when two devices attempt to transmit at exactly the same time. In addition, the lack of collisions allows switches to communicate with devices in full-duplex mode. In a full-duplex configuration, devices can send and receive data from the switch at the same time. Contrast this with half-duplex communication, in which communication can occur in only one direction at a time. The net result of these measures is that switches can offer significant performance improvements over hub-based networks, particularly when network use is high.

Bridges

A bridge is a device that allows for segmentation of a large network into two smaller, more efficient networks. If it is required to add an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can “listen” to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. The bridge is like a traffic constable at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling, or physical to-

pologies. They must, however, be used between networks with the same protocol.

Bridges can be used to reduce network congestion and improve performance by segmenting busy Ethernet networks into smaller collision domains. Bridges can also be used to connect segments more efficiently than repeaters and to join dissimilar networks such as Ethernet and token ring. Remote bridges can be used to create WAN links.

A poorly placed bridge can actually worsen network performance. For example, if a bridge is used to divide users who belong to the same department and frequently communicate with each other over the network, this might actually slow down communication among users by creating a bottleneck. It is better to use bridges to join separate departmental LANs together on which intra-departmental traffic is greater than interdepartmental traffic.

When using bridges to connect networks, make sure that only one path leads to any destination node on the network; otherwise, frames could become locked in loops and circle the network endlessly, causing a network storm.

Routers

A router translates information from one network to another. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even “listen” to the entire network to determine which sections are busiest – they can then redirect data around those sections until they clear up.

If a LAN is to be connected to the Internet, a router will be needed. In this case, the router serves as the translator between the information on the LAN and the Internet. It also determines the best route to send the data over the Internet. Routers can:

- Direct signal traffic efficiently
- Route messages between any two protocols
- Route messages between linear bus, star, and star-wired ring topologies
- Route messages across fiber optic, coaxial, and twisted-pair cabling

Routers work at the network layer (layer 3) of the Open Systems Interconnection (OSI) reference model for networking to move packets between networks using their logical addresses. Because routers operate

Module 2, Chapter 2

at a higher OSI level than bridges do, they have better packet-routing and filtering capabilities and greater processing power, which results in routers costing more than bridges.

Routers contain internal tables of information called routing tables that keep track of all known network addresses and possible paths throughout the internetwork, along with the cost of reaching each network. Routers route packets based on the available paths and their costs, thus taking advantage of redundant paths that can exist in a mesh topology network. Because routers use destination network addresses of packets, they work only if the configured network protocol is a routable protocol such as TCP/IP or IPX/SPX. This is different from bridges, which are protocol-independent.

Routing tables play a very important role in the routing process. They are the means by which the router makes its decisions. For this reason, a routing table needs to be two things. It must be up-to-date, and it must be complete. There are two ways that the router can get the information for the routing table—through static routing or dynamic routing.

Static routing

In environments that use static routing, routes and route information are entered into the routing tables manually. Not only can this be a time-consuming task, but errors are more common. Additionally, when there is a change in the layout, or topology, of the network, statically configured routers must be manually updated with the changes. Again, this is a time-consuming and potentially error-laden task. For these reasons, static routing is suited to only the smallest environments with perhaps just one or two routers. A far more practical solution, particularly in larger environments, is to use dynamic routing.

Dynamic routing

In a dynamic routing environment, routers use special routing protocols to communicate. The purpose of these protocols is simple; they allow routers to pass on information about themselves to other routers so that other routers can build routing tables. There are two types of routing protocols used—the older distance vector protocols and the newer link state protocols.

Gateways

Any device that translates one data format to another is called a gateway. Some examples of gateways include a router that translates data from one network protocol to another, a bridge that converts between two networking systems, and a software application that converts between two dissimilar formats. The key point about a gateway is that only the data format is translated, not the data itself. In many cases, the gateway functionality is incorporated into another device.

Gateways generally operate at the higher levels of the Open Systems Interconnection (OSI) reference model for networking. They are commonly used to provide connectivity between two different protocol stacks that might be running on different systems.

Examples include the following:

- ▶ **E-mail gateways**—for example, a gateway that receives Simple Mail Transfer Protocol (SMTP) e-mail, translates it into a standard X.400 format, and forwards it to its destination
- ▶ **Gateway Service for NetWare (GSNW)**, which enables a machine running Microsoft Windows NT Server or Windows 2000 Server to be a gateway for Windows clients so that they can access file and print resources on a NetWare server
- ▶ Gateways between a Systems Network Architecture (SNA) host and computers on a TCP/IP network, such as the one provided by Microsoft SNA Server
- ▶ A packet assembler/disassembler (PAD) that provides connectivity between a local area network (LAN) and an X.25 packet-switching network
- ▶ A gateway is usually a dedicated device or a set of services running on a dedicated computer. Gateways are essentially devices that direct network traffic in some fashion and translate information.

Network Operating Systems

Every network today uses some form of software to manage its resources. This software runs on a special, high-powered computer and is called a network operating system (or NOS, for short). The NOS is one of the most important components of the network. We will look at some of the most popular network operating systems:

- ▶ Novell NetWare
- ▶ Microsoft Windows NT, Windows 2000 Server
- ▶ Unix
- ▶ Linux
- ▶ Macintosh OS (Mac OS)

NetWare, developed by Novell, was the first network operating system to gain wide acceptance in the PC market. Windows NT, introduced by Microsoft in 1993, is gaining market share as of late because of its ease of use. Unix, while being the oldest network operating system, is only starting to gain popularity with PC users through PC-based flavors of Unix, such as Linux. This rise in popularity is due in part to the Internet, which is based on Unix standards and protocols. The fourth network operating system in use today—though used in a much smaller part of the networking market—is Apple's Macintosh OS, also known as the Mac OS.

Novell NetWare

A network operating system from Novell that is widely used in local area networks (LANs). NetWare was created by Novell in the early 1980s.

NetWare versions 2 and 3 were essentially used for LAN-based file and print servers running the Internetwork Packet Exchange (IPX) protocol that were administered by menu-driven MS-DOS-based utilities such as **SYSCON**, **FILER**, **FCONSOLE**, **PCONSOLE**, and **MONITOR**. NetWare 4 offers a more scalable solution by providing Novell Directory Services (NDS). The hierarchical NDS allows users to locate and access shared resources anywhere on the network regardless of their physical location. NDS supports the TCP/IP protocol and the Windows-based administration tool **NWADMIN**, which replaced most of the menu-driven MS-DOS-based administration tools for managing an entire NetWare 4-based network from a single location. NetWare 4 also supports single-network logon, in which users log on once to the NDS tree, are authenticated, and can then find and access all resources on the network for which they have appropriate permissions. Other internal system enhancements enable NetWare 4 to provide improved performance for file and print services.

NetWare 5, the latest version, includes support for native Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and a new multiprocessing kernel with virtual memory support.

Microsoft Windows NT, Windows 2000 Server

With the same graphical interface as other versions of Windows and simple administration possible from the server console, Windows NT is a force to be reckoned with. Because of its similarity to the Windows operating system and its powerful networking features, Windows NT gained popularity. Microsoft began to put its significant marketing resources behind it, and Windows NT became a viable alternative in the network operating system market previously dominated by Novell NetWare and the various flavors of Unix.

Windows NT

Windows NT was first released in 1993 in two versions—a server version called Windows NT Advanced Server and an associated client version called Windows NT 3.1. Windows NT includes such networking and security features as:

- ▶ NTFS file system for advanced local and remote file system security
- ▶ Windows NT domains, which are implemented using domain controllers for secure logons in a networking environment
- ▶ Trust relationships for building enterprise-level multi-domain networks

- ▶ Centralized storage of user profiles to support roaming users on the network
- ▶ Remote Access Service (RAS) for supporting remote users
- ▶ Support for both the server and client sides of Dynamic Host Configuration Protocol (DHCP) and Windows Internet Naming Service (WINS)
- ▶ Support for the software implementation of RAID levels 0, 1, and 5
- ▶ Integrated support for the TCP/IP protocol suite and associated utilities
- ▶ Services for Apple Macintosh
- ▶ Support for Novell NetWare migration

Windows 2000 Server

A comprehensive application, file, print, and Internet services platform that replaces Windows NT Server and provides increased reliability, scalability, management, and applications support. Its features include the following:

- ▶ Active Directory, a directory service based on the X.500 directory specifications that simplifies centralized, one-point management of distributed network resources.
- ▶ Windows Management Tools, which are snap-ins for the Microsoft Management Console (MMC). MMC provides a unified interface for managing enterprise-level network resources.
- ▶ Enhanced Internet services, including Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP) server support through Internet Information Services (IIS).
- ▶ Windows Terminal Services for running terminal emulation on thin clients, replacing Windows NT Server, Terminal Server Edition.
- ▶ Support for Kerberos and public key infrastructure (PKI) security services.

Unix

An operating system developed at AT&T Bell Laboratories in 1969 and widely deployed today in the enterprise networking environment. UNIX was the first operating system written entirely in the C programming language and consequently has close ties to C.

UNIX was designed as a time-sharing environment, in contrast to the batch environment of most computing systems of the time. Using UNIX, multiple users could simultaneously access the system and run their programs, communicating interactively with the system using remote terminals. Users could thus collaborate in real time on computing projects by sharing files and resources.

Module 2, Chapter 2

UNIX became widely available around 1975 and established strong roots in academic computing environments, where it is still used and taught today. UNIX has the stability and robustness of an operating system that has evolved over 25 years, but it has a reputation for being difficult to learn and administer. UNIX has evolved into a number of different “flavors” as vendors have adapted it to their own hardware platforms. These flavors include the following:

- ▶ **System V:** Evolved from versions of UNIX developed by UNIX Systems Laboratories and AT&T
- ▶ **BSD:** Developed at the University of California, Berkeley; the basis of the SunOS from Sun Microsystems
- ▶ **AIX:** Developed by IBM for its mid-range computer systems
- ▶ **HP/UX:** Developed by Hewlett-Packard
- ▶ **Solaris:** Developed by Sun Microsystems for its SPARC systems
- ▶ **IRIX:** Developed by Silicon Graphics for its high-end workstations

The original source code for System V UNIX is owned by Santa Cruz Operation (SCO), which licenses the code to other UNIX vendors and offers its own version called SCO UNIX for various hardware platforms. The actual trademark “UNIX” is now owned by The Open Group, a consortium of software and hardware manufacturers. A variety of open versions of UNIX also exist. These are highly popular machine-independent implementations of UNIX that have been compiled to run on multiple hardware platforms. Their source code is available with few restrictions. An example is FreeBSD, which evolved from BSD UNIX. Another example is Linux, a UNIX-like operating system that is rapidly growing in popularity.

Linux

The Unix flavor that has been receiving the most attention lately is Linux. Linux is a fairly easy-to-use flavor whose kernel was developed by Linus Torvalds at the University of Helsinki, Finland. He started his work in 1991 and released version 1 of the Linux kernel in 1994. At the time of this writing, the current Linux kernel is version 2.2.

Linux runs mainly on the Intel platform, although some distributions run on RISC processors such as the MIPS and Alpha. Attempts have been made, successfully, to run the RISC version on other platforms, such as the Macintosh. Linux is easy to install, and most distributions are free and include the source code. Hardware requirements can vary widely with each distribution. Today, Linux can run on hardware ranging from mobile phones to mainframes!

And there are various flavors of Linux. People acquire Linux, come up with a new feature, recompile Linux with the new feature, and then re-distribute Linux. According to Linux’s distribution agreement (called

the GNU public license), any sale or distribution must include the source code so that others can also develop custom Linux applications.

Most Linux distributions include a full suite of applications, such as word processors, the X Window graphical interface and compilers. Additionally, most Unix applications that comply with the POSIX standard should run on Linux with little or no modification. Because Linux is a flavor of Unix, it comes with network support for TCP/ IP. In particular, Caldera's OpenLinux is making its mark in the networking world. OpenLinux was developed for corporate networking, so it supports multiple protocols (including PPP [Point-to-Point Protocol], AppleTalk, IPX, and SMB). It also includes support for integration with other network operating systems. Red Hat produce Linux CD distributions that are oriented around simple management and total upgradability. Red Hat includes graphical and web based configuration tools, RPM package management, and extensive multiplatform support. LSB compliance with errata packages. SuSE produce a very comprehensive English and German language CD-ROM distribution and a collection of archive CD's. They also provide German and English language support and applications.

Macintosh

The Macintosh interface is considered to be the easiest to use, of all graphical user interfaces. Developed in 1983, the Macintosh OS (or Mac OS) is seeing a resurgence of popularity with the introduction of several new models, like the iMac, the G4 cube, and the Titanium PowerBook G4 Macintosh. Macintosh has always had a very loyal following, and with good reason. The Macintosh OS (combined with the Macintosh hardware platform) is very user-friendly. As such, many people who have never used computers before are buying Macs.

Summary

This chapter takes the reader through more details on network - the physical aspects: the cables and other components. The Chapter also details different operating systems that are available on the network. From an audit perspective, understanding the function of each one of these is important so that their vulnerabilities and remedial control measures can be understood.



3 Network Design and Maintenance

✂ Learning Goals ✂

The chapter familiarizes the reader with

- ▶ Different types of networks such as single, two and three tier architectures and associated concepts of fat and thin client and their relative advantages and disadvantages: this should help the reader in assessing the suitability of architectures for different applications
- ▶ Different wide area networking technologies and accessories
- ▶ Activities associated with network management

Principles of Network Design

Client/Server (C/S) is a general description of a networked system where a client program initiates contact with a separate server program (usually on a different machine) for a specific function or purpose. The client exists in the position of the requester for the service provided by the server.

As large scale, complex information systems have evolved over the past two decades, the Client/Server model of computing has come to be generally accepted as the preferred architecture for application design and deployment.

The term Client/Server has traditionally been associated with a desktop PC connected over a network to some sort of SQL-database server. In fact, the term Client/Server formally refers to a logical model that provides for a division of tasks into 'client' and 'server' layers or 'tiers'.

One-Tier Monolithic Client/Server Architectures

The Information Technology (IT) industry, have been practising a simple form of Client/Server computing since the inception of the mainframe. That configuration, a mainframe host and a directly connected (unintelligent) terminal constitutes a one-tier C/S system.

Two-Tier Client/Server Architectures

In a two-tier client/server architecture, the client communicates directly with the database server. The application or business logic either resides in the client or in the database server in the form of stored procedures.

A two-tier (C/S) model first began to emerge with the applications developed for local area networks in the late eighties and early nineties, and

Module 2, Chapter 3

was primarily based upon simple file sharing techniques implemented by X-base style products (dBase, FoxPro, Clipper, Paradox, etc.).

Fat Clients

The two-tier model initially involved a non-mainframe host (a network file server), and an intelligent “fat client” where most of the processing occurs. The term “fat client” is used to indicate the mean that the client has large resources, in the form of CPU power, memory and disk space. This configuration did not scale well however, to facilitate large or even mid-size information systems (greater than 50 or so connected clients).

Then the Graphical User Interface (GUI) emerged as the dominant environment for the desktop. With it, emerged a new slant on the early two-tier architecture. The general purpose LAN file server was replaced by a specialized database server. This model spawned the emergence of new development tools: PowerBuilder, Visual Basic and Delphi to name a few.

Much of the processing still occurred on the “fat clients”, but datasets of information were delivered to the client using Structured Query Language (**SQL**) techniques to perform requests from a database server, which simply reported the results of queries.

The more complex the application, the fatter the client becomes and the more powerful the client hardware must be to support it. This increases the cost to a prohibitive level.

The bandwidth required for a fat client architecture is very large, thus reducing the number of users who can effectively use the network.

Fat Servers

Another approach that is used in the 2-tiered architecture as an alternative to the “fat client” model is the “thin client” or “fat server” configuration, where the user invokes procedures stored at the database server. In this architecture, the demand placed on the network bandwidth is lesser, resulting in a better performance.

The downside is stored procedures require proprietary customization and coding as they rely on the vendor’s procedural functionality. In addition, because stored procedures are embedded within the database, each database that contains the procedure must be modified when business logic changes. In a large distributed database, this can lead to difficult version management issues.

In both cases, remote database transport protocols such as SQL-Net are used to carry the transaction. In these models, a “heavy” network process is required to mediate the Client/Server interaction. Furthermore,

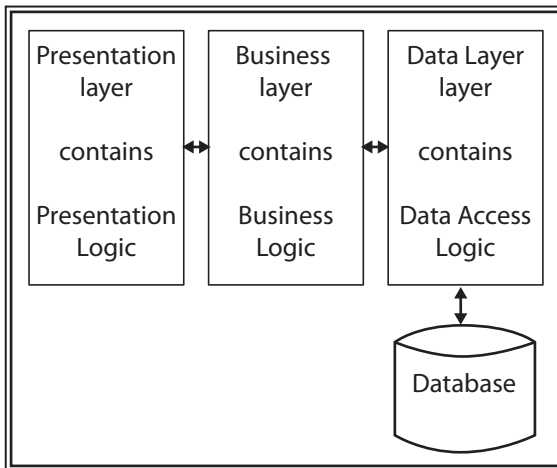
not only network transaction size, but query transaction speed is slowed down by this heavy interaction.

No matter which technique was used, two-tier (C/S) systems could still not scale beyond approximately 100 users. Overall, these architectures are typically NOT well suited for mission critical applications.

Three-Tier Client/Server Architectures

A newer generation of Client/Server implementations takes this segmented model a step further and adds a middle tier to achieve a '3-tier' architecture.

Figure 1: Three-Tier Client/Server Architecture



In a three-tier or multi-tier environment, the client implements the presentation logic (thin client). The business logic is implemented on application server(s) and the data resides on database server(s).

A Multi-tier architecture is thus defined by the following three component layers:

1. A front-end component, which is responsible for providing portable presentation logic;
2. A back-end component, which provides access to dedicated services, such as a database server.
3. A middle-tier component, which allows users to share and control business logic by isolating it from the actual application;

The advantages of Multi-Tier Client/Server architectures are:

- Changes to the user interface or to the application logic are largely independent of each other, allowing the application to evolve easily to meet new requirements.

Module 2, Chapter 3

- ▶ Network bottlenecks are minimised because the application layer does not transmit extraneous data to the client, only data needed to handle a task is transmitted.
- ▶ When business logic changes are required, only the server has to be updated. In two-tier architectures, each client must be modified when logic changes.
- ▶ The client is insulated from database and network operations. The client can access data easily and quickly without having to know where data resides or how many servers are on the system.
- ▶ Database connections can be 'pooled' and thus shared by several users, which greatly reduces the cost associated with per-user licensing.
- ▶ The organization has database independence because the data layer is written using standard SQL which is platform independent. The enterprise is not tied to vendor-specific stored procedures.
- ▶ The application layer can be written in standard third or fourth generation languages, such as Java, C or COBOL, with which the organization's in-house programmers are experienced.

Fat Middle

A multi-tier architecture augments traditional client/server and two-tier computing by introducing (one or more) middle-tier components.

The client system interacts with the middle-tier via a standard protocol such as HTTP or Remote Procedure Calls (RPC). The middle-tier interacts with the backend server via standard database protocols such as SQL, ODBC and JDBC.

This middle-tier contains most of the application logic, translating client calls into database queries and other actions, and translating data from the database into client data in return.

This placement of business logic on the application server provides scalability and isolation of the business logic in order to handle rapidly changing business needs. In addition, this allows a more open choice of database vendors.

The 3-tier architecture can be extended to N-Tiers when the middle-tier provides connections to various types of services, integrating and coupling them to the client, and to each other.

N-Tier Architectures (Thin all over)

As the Client/Server model continued to evolve, more sophisticated multi-tier solutions appeared, where client-side computers began to operate as both clients and servers.

This latest refinement of the Client/Server model came when software developers recognized that the smaller, specialized processes were easier to design, faster to implement and cheaper to maintain.

These same principles were in turn, applied to the server side of the configuration, resulting in smaller, specialized server processes.

Today, the industry appears to be rapidly moving toward a N-Tier architecture. The majority of new IS development is typically being written as an N-Tier C/S system of some kind.

N-Tier architecture do not preclude the use of the two-tier or three-tier model. Depending on the scale of the application and the requirements for access to data, the two- or three-tiered model can be used for departmental applications.

It does not make sense to force a client's reporting needs to go through the application server when there is no requirement for transactional integrity in ad-hoc reporting. In this situation, the client should be able to access the data directly from the database server.

N-Tier computing is usually considered the most effective approach because it can provide integration of current information technology into this new, more flexible model.

Advantages of N-Tier Architecture

True Distributed Computing

Today, the Network (Internet, Intranet and Extranet) is the computer. This fundamental change in computing models brings both challenges and opportunities like never before.

N-Tier based architectures allow business components to run on a LAN, WAN, or the Internet - a truly distributed computing environment. This means that anyone with a computer and Internet access - for example: a sales person with a laptop away from the office - has all of the functionality available that in-house users have on their desktop systems.

N-Tier distributed component technology is essential for building the next generation of e-business related applications — applications that are highly scalable and reliable, while providing high throughput and seamless integration with back-end legacy systems.

Next-Generation Technology

Enterprise-class N-Tier architectures are becoming the new foundation for developing mission-critical applications and offer the only workable architecture for next-generation Internet-based distributed computing solutions.

N-Tier distributed computing systems provide an unmatched set of technological advances such as: connection pooling, connection multiplexing, dynamic load balancing and superb performance on clustered hardware.

Module 2, Chapter 3

N-Tier industrial-strength applications can help companies develop new core competencies in everything from knowledge management to electronic commerce related systems, all the while implementing the scalable technology of the future.

The Application Development Strategy for the 21st Century

N-Tier is not a product or a standard, but rather a **STRATEGIC CONCEPT** on how to logically construct and deploy an adaptable distributed computer system.

Partitioned N-Tiered systems help facilitate rapid application development and deployment advantages with incremental benefits delivered through co-ordinated parallel development efforts and smart outsourcing, resulting in greatly decreased development time and related costs.

Many e-business applications now use a simple HTML based browser as a universal “**THIN-CLIENT**” interface. A thin-client based architecture places the visual or presentation layer of the application on the client system, while the business logic and data reside on the middle and server tiers. Designing for thin-clients greatly minimizes application deployment problems while maximizing user accessibility from a wide variety of platforms.

N-Tier application frameworks are built to take advantage of **OPEN INDUSTRY STANDARDS** which allow the resulting applications to operate in distributed, cross-platform environments. Using these powerful “**OPEN STANDARDS**” allows System Integrators to ensure effective and consistent inter-departmental and inter-enterprise capable, cross-application communication and messaging at all levels.

WAN Technologies

A WAN is a data communications network that covers a relatively broad geographic area and often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

Point-to-Point Links

Also called a leased line or dedicated line, a telecommunications service provided to businesses by “telcos” (telecommunication companies) and long distance carriers that provides a permanent direct connection between two geographically separate local area networks (LANs). Leased lines are dedicated circuits that the telco reserves for the exclusive use of the customer. They are permanently available, always active, and secure, and they have a consistent quality of service (QoS) and a flat monthly fee. However, they are very expensive compared to dial-up lines, and

businesses rarely use their full bandwidth capabilities except in short bursts.

Leased lines are a form of point-to-point connection. The LAN is connected to the telco's central office (CO), which sets up dedicated switches to connect to the destination LAN. The presence of dedicated switches is what makes leased lines so expensive. Since the leased line is always on, there is no connection delay when users try to access the server for their e-mail.

Leased lines are available in 64 Kbps and its multiples, like 128 Kbs, 2 Mbs, etc. They are used mainly for connecting customer premises to the telco central office. The charge for a leased line is based on both bandwidth and distance; leased lines are usually leased for a base monthly cost, and sometimes incur an extra monthly charge proportional to the traffic carried on the line.

Message Switching

In message switching a complete message is sent to a concentration point for storage and routing to the destination point when a communication path is available. Transmission cost is based on message length.

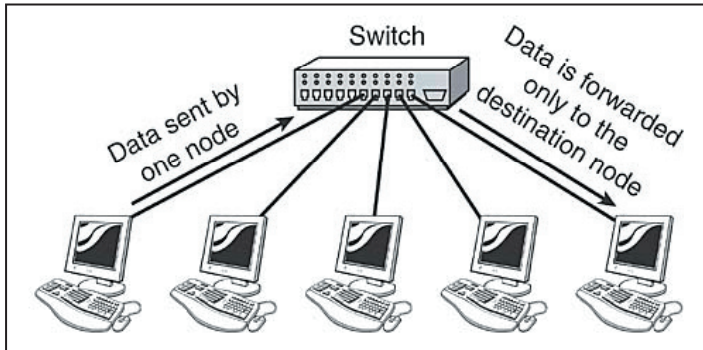
Circuit Switching

A telecommunications service provided to businesses by telcos and long-distance carriers. "Circuit-switched services" is an umbrella term describing any service that provides switched connections between a consumer and a provider. The telephone system is an example of a circuit-switched service. Circuit-switched services are temporary circuits only, and can be contrasted with leased lines, which use dedicated switches.

With circuit-switched services, a new switched circuit must be established each time one local area network (LAN) attempts to connect to a remote LAN. Different switches can be used for each attempt, depending on availability and traffic, so the quality of services can vary between connections. The LAN is connected through devices to the telco's central office (CO), which sets up switches on demand to connect to the destination LAN. When the wide area network (WAN) link is disconnected, the switches are freed up for other purposes.

A circuit-switched WAN undergoes a process similar to that used for a telephone call.

Figure 3: Circuit switched WAN



WAN Virtual Circuits

A virtual circuit is a logical circuit created to ensure reliable communication between two network devices. Two types of virtual circuits exist: **SWITCHED VIRTUAL CIRCUITS (SVCS) AND PERMANENT VIRTUAL CIRCUITS (PVCs)**.

SVCs are virtual circuits that are dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the virtual circuit between the source and destination devices. Data transfer involves transmitting data between the devices over the virtual circuit, and the circuit-termination phase involves tearing down the virtual circuit between the source and destination devices. SVCs are used in situations in which data transmission between devices is sporadic, largely because SVCs increase bandwidth used due to the circuit establishment and termination phases, but decrease the cost associated with constant virtual circuit availability.

A PVC is a permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of virtual circuits, but increase costs due to constant virtual circuit availability.

Packet Switching

The process by which a networking or telecommunications device accepts a packet and switches it to a telecommunications device that will take it closer to its destination. Packet switching allows data to be sent over the telecommunications network in short bursts or "packets" that contain sequence numbers so that they can be reassembled at the destination. Wide area network (WAN) devices called switches route packets from one point on a packet-switched network to another. Data within

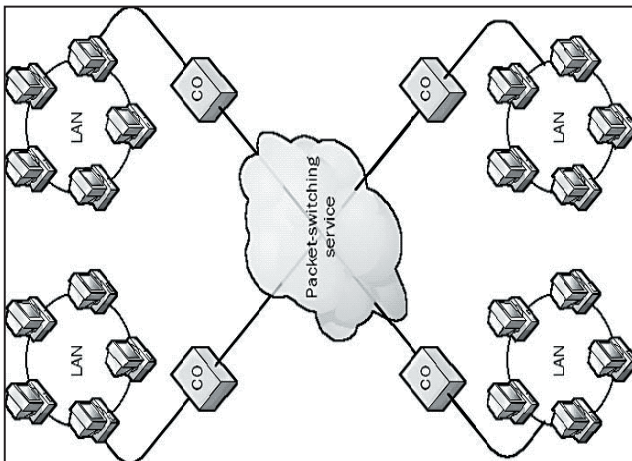
the same communication session might be routed over several different paths, depending on factors such as traffic congestion and switch availability.

Packet switching is the transmission method used for most computer networks because the data transported by these networks is fundamentally “bursty” in character and can tolerate latency (due to lost or dropped packets). In other words, the transmission bandwidth needed varies greatly in time, from relatively low traffic because of background services such as name resolution services, to periods of high bandwidth usage during activities such as file transfer. This contrasts with voice or video communication, in which a steady stream of information must be transmitted in order to maintain transmission quality and in which latency must remain minimised to preserve intelligibility. (Latency is defined as the amount of time it takes a packet to travel from source to destination.)

The Internet is the prime example of a packet-switched network based on the TCP/IP protocol suite. A series of routers located at various points on the Internet’s backbone forward each packet received on the basis of destination address until the packet reaches its ultimate destination. TCP/IP is considered a connectionless packet-switching service because Transmission Control Protocol (TCP) connections are not kept open after data transmission is complete.

Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Service (SMDS), and X.25 are examples of packet-switched WAN technologies.

Figure 3: Packet Switched WAN



The packeting process varies with the particular service used, but it basically consists of breaking down network message into relatively small

Module 2, Chapter 3

individual packets of data and tagging the packets with the destination address of the remote node to which the packet is directed. Each end node (local network access device) connected to the cloud has a layer 2, or data-link layer, address that is known to every other end node. These addresses are used to route packet data between individual nodes on the WAN or to broadcast packets to all nodes when needed. Other information is also tagged onto the packets for error correction and other purposes, depending on the service used. The packets are usually small to lessen the load on the switching devices and to enable quick retransmission when transmission errors occur.

Packets are individually placed onto the carrier's packet-switched network and switched from circuit to circuit until they reach their destination. Two packets forming part of the same network message might take entirely different routes to reach their destination node—it depends on the best route available at any given moment, as determined by the packet-switching services themselves. This is different from circuit-switched networks, in which all data are sent over the same switched circuits for the duration of the connection. At the destination, the packets are re-assembled into network frames and delivered to the remote network, where they are routed to their destination computers.

In networking diagrams, a public packet-switched network is typically depicted as a cloud because the details of the switches and connections are not of interest to the customer—they are the responsibility of the carrier or carriers providing the services.

Advantages of packet-switching services include the following:

- ▶ Customers are not restricted to a single destination, as with point-to-point connections using leased lines.
- ▶ Packets can be routed to any destination that supports similar services, so businesses are not tied to a particular carrier or telco.
- ▶ Packet-switched networks have low latency and are suitable for hosting dedicated services such as company Web servers if the connection has sufficient bandwidth.
- ▶ Customers usually pay monthly rates plus additional charges based on bandwidth use, which means that the primary charges are on a per-transaction basis.

WAN Dialup Services

Dialup services offer cost-effective methods for connectivity across WANs. Two popular dialup implementations are dial-on-demand routing (DDR) and dial backup.

DDR is a technique whereby a router can dynamically initiate and close a circuit-switched session as transmitting end station demand.

Dial backup is a service that activates a backup serial line under certain conditions. The secondary serial line can act as a backup link that is used when the primary link fails or as a source of additional bandwidth when the load on the primary link reaches a certain threshold. Dial backup provides protection against WAN performance degradation and downtime.

WAN Devices

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, modems, CSU/DSUs, and ISDN terminal adapters are discussed in the following section. Other devices found in WAN environments that are exclusive to WAN implementations include routers, ATM switches, and multiplexers.

WAN Switch

A WAN switch is a multi-port internetworking device used in carrier networks. These devices typically switch such traffic as Frame Relay, X.25, and SMDS and operate at the data link layer of the OSI reference model.

Access Server

An access server acts as a concentration point for dial-in and dial-out connections. For example, a number of user computers could be connected to modems and the modems connected to one Access Server. The Access Server would be then connected by a high-speed link to the Internet.

Modem

A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, these analog signals are returned to their digital form.

CSU/DSU

A channel service unit/digital service unit (CSU/DSU) is a digital-interface device (or sometimes two separate digital devices) that adapts the physical interface on a data terminal equipment (DTE) device (such as a terminal) to the interface of a data circuit-terminating (DCE) device (such as a switch) in a switched-carrier network. The CSU/DSU also provides signal timing for communication between these devices.

SDN Terminal Adapter

An ISDN terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces, such as EIA/TIA-232. A terminal adapter is essentially an ISDN modem.

Multiplexers

A **MULTIPLEXER** is a physical layer device that combines multiple data streams into one or more output channels at the source. Multiplexers demultiplex the channels into multiple data streams at the remote end and thus maximize the use of the bandwidth of the physical medium by enabling it to be shared by multiple traffic sources. Some methods used for multiplexing data are time-division multiplexing (TDM), asynchronous time-division multiplexing (ATDM), frequency-division multiplexing (FDM), and statistical multiplexing.

In TDM, information from each data channel is allocated bandwidth based on preassigned time slots, regardless of whether there is data to transmit. In ATDM, information from data channels is allocated bandwidth as needed by using dynamically assigned time slots. In FDM, information from each data channel is allocated bandwidth based on the signal frequency of the traffic. In statistical multiplexing, bandwidth is dynamically allocated to any data channels that have information to transmit.

Network Management

NETWORK MANAGEMENT means different things to different people. In some cases, it involves a solitary network consultant monitoring network activity with a protocol analyzer. In other cases, network management involves a distributed database, auto-polling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, network management is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks.

A Historical Perspective

The early 1980s saw tremendous expansion in the area of network deployment. As companies realized the financial benefits and productivity gains created by network technology, they began to add networks and expand existing networks almost as rapidly as new network technologies and products were introduced. By the mid-1980s, certain companies were experiencing difficulties from deploying many different (and sometimes incompatible) network technologies.

The problems associated with network expansion affect both day-to-day network operation management and strategic network growth planning. Each new network technology requires its own set of experts. In the early 1980s, the staffing requirements alone for managing large, heterogeneous networks created a crisis for many organizations. An urgent need arose for automated network management (including what is typically called network capacity planning) integrating diverse environments.

Network Management Architecture

Most network management architectures use the same basic structure and set of relationships. End stations (managed devices), such as computer systems and other network devices, run software that enables them to send alerts when they recognize problems (for example, when one or more user-determined thresholds are exceeded). Upon receiving these alerts, management entities are programmed to react by executing one, several, or a group of actions, including operator notification, event logging, system shutdown, and automatic attempts at system repair.

Management entities also can poll end stations to check the values of certain variables. Polling can be automatic or user-initiated, but agents in the managed devices respond to all polls. Agents are software modules that first compile information about the managed devices in which they reside, then store this information in a management database, and finally provide it (proactively or reactively) to management entities within network management systems (NMSs) through a network management protocol.

Well-known network management protocols include the Simple Network Management Protocol (SNMP) and Common Management Information Protocol (CMIP). Management proxies are entities that provide management information on behalf of other entities.

ISO Network Management Model

The ISO has contributed a great deal to network standardization. Its network management model is the primary means for understanding the major functions of network management systems. This model consists of five functions, as discussed in the next sections.

Performance Management

The goal of **PERFORMANCE MANAGEMENT** is to measure and make available various aspects of network performance so that internetwork performance can be maintained at an acceptable level. Examples of performance variables that might be provided include network throughput, user response times, and line utilization.

Performance management involves three main steps. First, performance data is gathered on variables of interest to network administrators. Second, the data is analyzed to determine normal (baseline) levels. Finally, appropriate performance thresholds are determined for each important variable so that exceeding these thresholds indicates a network problem worthy of attention.

Management entities continually monitor performance variables. When a performance threshold is exceeded, an alert is generated and sent to the network management system.

Module 2, Chapter 3

Each of the steps just described is part of the process to set up a reactive system. When performance becomes unacceptable because of an exceeded user-defined threshold, the system reacts by sending a message. Performance management also permits proactive methods: For example, network simulation can be used to project how network growth will affect performance metrics. Such simulation can alert administrators to impending problems so that counteractive measures can be taken.

Configuration Management

The goal of **CONFIGURATION MANAGEMENT** is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

Each network device has a variety of version information associated with it. An engineering workstation, for example, may be configured as follows:

- ▶ Operating system, Version 3.2
- ▶ Ethernet interface, Version 5.4
- ▶ TCP/IP software, Version 2.0
- ▶ NetWare software, Version 4.1
- ▶ NFS software, Version 5.1
- ▶ Serial communications controller, Version 1.1
- ▶ X.25 software, Version 1.0
- ▶ SNMP software, Version 3.1

Configuration management subsystems store this information in a database for easy access. When a problem occurs, this database can be searched for clues that may help solve the problem.

Accounting Management

The goal of accounting management is to measure network utilization parameters so that individual or group uses on the network can be regulated appropriately. Such regulation minimizes network problems (because network resources can be apportioned based on resource capacities) and maximizes the fairness of network access across all users.

As with performance management, the first step towards appropriate accounting management is to measure utilization of all important network resources. Analysis of the results provides insight into current usage patterns, and usage quotas can be set at this point. Some corrections, of course, will be required to reach optimal access practices. From this point, ongoing measurement of resource use can yield billing information as well as information used to assess continued fair and optimal resource utilization.

Fault Management

The goal of **FAULT MANAGEMENT** is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.

Fault management involves first determining symptoms and isolating the problem. Then the problem is fixed and the solution is tested on all important subsystems. Finally, the detection and resolution of the problem are recorded.

Security Management

The goal of **SECURITY MANAGEMENT** is to control access to network resources according to local guidelines so that the network cannot be made to fail (intentionally or unintentionally) and sensitive information cannot be accessed by those without appropriate authorization. A security management subsystem, for example, can monitor users logging on to a network resource and can refuse access to those who enter inappropriate access codes.

Security management subsystems work by partitioning network resources into authorized and unauthorized areas. For some users, access to any network resource is inappropriate, mostly because such users are usually company outsiders. For other (internal) network users, access to information originating from a particular department is inappropriate. Access to Human Resource files, for example, is inappropriate for most users outside the Human Resources department.

Security management subsystems perform several functions. They identify sensitive network resources (including systems, files, and other entities) and determine mappings between sensitive network resources and user sets. They also monitor access points to sensitive network resources and log inappropriate access to sensitive network resources.

Network Management Solutions

Some examples of products used for Network Management tasks are

- ▶ **Cisco WAN Manager:** Cisco WAN Manager (CWM) is a network and element management system that enables operations, administration, maintenance of WAN multiservice networks.
- ▶ **NetBeacon Element Management System:** NetBeacon provides network management that graphically shows all link connections, environmental conditions, port activity and status at a glance
- ▶ **Concord Communications eHealth QoS:** QoS enables service providers and enterprises to offer different classes of service, with different

performance commitments, across the same physical infrastructure.

- ▶ **ManageEngine OpManager:** ManageEngine OpManager is a comprehensive Network, System and Application monitoring software that offers advanced network monitoring functionality at an affordable price.

Network Monitoring Tools

In an enterprise's networking environment, a number of tools are used to manage and monitor the network. These can be enumerated as follows:

- ▶ **Downtime Reports:** Used for tracking the working of telecommunication lines and devices. Interruptions due to power failure, operator error, traffic overloading, or possible interception of transmissions are identified in this report.
- ▶ **Response time reports:** These reports typically identify average, worst and best response times over a given time interval for individual telecommunications lines or systems. If response time is slow all possible causes such as intermediate networking device speeds, network configuration, etc. should be analyzed.
- ▶ **Online monitors:** Measure telecommunications transmissions and determine whether transmissions are accurate and complete. Monitoring capabilities include echo checking, which transmits back to the sending station for verification and status checking of all transmissions, which ensures that messages are not lost or transmitted more than once.
- ▶ **Protocol analyzers:** They are hardware or software devices offering various network troubleshooting features, including protocol-specific packet decodes, specific preprogrammed troubleshooting tests, packet filtering, and packet transmission.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is most often used for collecting statistical and configuration information about network devices such as computers, hubs, switches, routers, and even network printers. The statistical information includes the number of packets or frames sent or received per second, the number of errors per second, and so on. The configuration information includes the IP address of an interface on the device, the version of the operating system running on the device, and so on. Management systems are used to monitor network health, trap errors, perform diagnostics, and generate reports. SNMP is the most popular network management protocol in use.

Network Monitor

A Microsoft Windows 2000 and Windows NT administrative tool that functions as a software-based network packet analyzer for troubleshooting network problems. The Network Monitor can be used to

- ▶ Capture data frames from a connected network
- ▶ Display, filter, edit, and retransmit frames on the network
- ▶ Monitor and display protocol statistics
- ▶ Examine individual captured frames in detail

Data Backup and Recovery Strategies

Data recovery depends on the methods for performing a backup of files and directories. Each type of backup has a different function in an overall backup plan. Most network backup software supports five backup methods:

Normal backup

Backs up everything that is selected to be backed up. Normal backups are the easiest to restore. Normal backups are sometimes referred to as “full backups.” A normal backup is used when all critical system and data files are to be backed up in a single operation. If the back-up cycle consists of only normal back-up, during recovery, only the most recent normal back-up needs to be restored.

Copy backup

Primarily used to produce an additional copy of a backup—for example, a copy to send to the accounting department for monthly archiving and reporting. While a copy backup backs up the same files as a normal backup, there is a difference between the two operations. Performing a normal backup clears the archive bit on each backed up file and marks them as having been backed up. A copy backup, however, does not modify the archive bit on the files backed up. In other words, a copy backup can be performed at any time in a backup cycle without interrupting the cycle in any way—the copy backup is distinct from the backup cycle and is not required when a restore is performed from the cycle’s set of tapes.

Incremental backup

Backs up only files that have been created or modified since the last normal or incremental backup. Files that are backed up in an incremental backup have their archive attributes cleared to indicate that they have been backed up. Using a combination of normal and incremental backups takes less time and uses less storage space than performing only normal backups. However, if restoration needs to be performed, typically the normal backup plus every incremental backup from the current backup cycle would be required.

Differential backup

Copies those files that have been created or changed since the last normal or incremental backup. Files that are backed up by a differential backup do not have their archive attributes cleared, which means that these files will be backed up again in any succeeding differential backups. Differential backups are cumulative with regard to changes—that is, each differential backup in a given backup cycle contains all the files from the last differential backup, plus any files that have been modified since the last differential backup. Thus, for restoration, the normal backup and the most recent differential backup from the current backup cycle would be required.

Daily copy backup

Copies all files that have been modified on the day the daily copy backup is performed. This method is sometimes used to make a copy of all files a user worked on in a day so that he or she can take them home to work on. Like a copy backup, the daily copy backup does not modify the archive bit of the files backed up; therefore, the daily copy backup does not interrupt the backup cycle in any way.

Storage Area Networks

A SAN is a storage area network—a collection of hard disks in a dedicated, very fast network, connected to servers via multiple switches. The SAN network is called a fabric, and connects any server to any storage device.

SANs are designed to be very reliable, very scalable, and very flexible. More storage can be added without disrupting operations, a number of backup schemes can be used that don't load the main network, and the SAN can be expected to manage very large data collections that span multiple disks. There are a wide variety of SAN switches, routers, and arrays available from a number of vendors. SANs can also be physically spread over whatever distance their network allows—kilometers with fiber-based systems—which can be a highly robust configuration.

A SAN Network

The most popular is Fibre Channel, although iSCSI, Gigabit Ethernet and IP over Fibre Channel (FCIP) are alternatives. Typically, switches run at 2 Gbps. Regardless of the physical layer, it's important to remember that a SAN is a network in its own right and has the same management and security issues as any business-critical LAN. In particular, structuring the internal SAN network into separate zones with different access privileges and physical configurations can enhance security and reliability.

Network Attached Storage (NAS)

NAS — network attached storage — connects storage devices to servers over a network, but leaves the storage management as a one-on-one relationship between server and storage. NAS systems can be combined with SANs by using a NAS head.

Summary

This chapter discusses the architectural issues: type of architectures, the advantage and disadvantage of each architecture. This will help the reader plan networks.

More sophisticated concepts such as switching techniques are introduced in this chapter. Having familiarized the reader with all the basic devices, more advanced devices are introduced in this chapter. By now, the reader should be fully proficient to understand any network s/he audits.

This is considered to be the appropriate time to introduce management issues. A student of audit should look at each of these management aspects from control perspective.

A peep into future technologies is also given with a view to make the auditor obsolescence proof.



4 Internet

✂ Learning Goals ✂

This chapter gives an insight into the following aspects of the Internet:

- Introduction to the Internet
- Internet Infrastructure and Protocols
- Internet Addressing
- Internet Services

Introduction to the Internet

Introduction

The Internet is a computer internetwork made up of thousands of networks worldwide. No one knows exactly how many computers are connected to the Internet. It is certain, however, that these number in millions.

No one is in charge of the Internet. There are organizations that develop technical aspects of this network and set standards for creating applications on it, but no governing body is in control. The Internet backbone, through which Internet traffic flows, is owned by private companies.

All computers on the Internet communicate with one another using the Transmission Control Protocol/Internet Protocol suite, abbreviated to TCP/IP. Computers on the Internet use a client/server architecture. This means that the remote server machine provides files and services to the user's local client machine. Software can be installed on a client computer to take advantage of the latest access technology.

An Internet user has access to a wide variety of services: electronic mail, file transfer, vast information resources, interest group membership, interactive collaboration, multimedia displays, real-time broadcasting, shopping opportunities, breaking news, and much more.

The Internet consists primarily of a variety of access protocols. Many of these protocols feature programs that allow users to search for and retrieve material made available by the protocol.

History of the Internet

In the 1960s during the cold war, an American defence research organisation decided to set up a computer network that would be able to re-route information. The resulting network was called ARPANET - Advanced Research Projects Agency Network.

Module 2, Chapter 4

In the 1970's the National Science Foundation (NSF) began funding the installation of supercomputers at major American universities. The demand by other universities to connect to this network began with the increasing amount of information stored in the network. Using high-speed telephone lines, the NSF began to connect its own supercomputers to facilitate the ready exchange of information. The result, NSFNET, grew to include many computers from various educational institutions across the United States.

The NSFNET, ARPANET, and other networks including USENET and BITNET, were all separate and could not communicate with one another. However, in the late 1980s they began to merge into what would eventually form the backbone of the Internet. Up until the early 1990's, the vast majority of Internet users were individuals at government agencies and educational institutions.

Companies including MCI, IBM, and Sprint began to gain interests in the Internet, and in May 1995, the NSF terminated its funding of the NSFNET backbone. Since then, the Internet has been largely in the hands of private industry, which in turn, responds to the market pressure of consumers.

Internet Organisations

As stated above, the Internet is not owned by any one group; it is a collection of networks and gateways that run a common TCP/IP protocol and that all evolved from ARPANET. Nevertheless, various administrative bodies oversee various aspects of the Internet. These groups include the following:

- ▶ Internet Society (ISOC), which co-ordinates a number of other bodies and gives advice and direction to them.
- ▶ Internet Architecture Board (IAB) which is responsible to the ISOC and oversees the architecture of the Internet.
- ▶ Internet Engineering Task Force (IETF), which is responsible to the IAB and develops Internet protocols that define the TCP/IP protocol suite, the Domain Name Service (DNS), and so on.
- ▶ Internet Assigned Numbers Authority (IANA), which is now replaced by the Internet Corporation for Assigned Names and Numbers (ICANN) ICANN was responsible for co-ordinating the registration of DNS names and assigning IP addresses.

Internet Infrastructure

Every computer that is connected to the Internet is part of a network. For example, a person would typically need to connect to an Internet Service Provider (ISP) to connect to the Internet. The ISP may then connect to a larger network and become part of their network. The Internet is simply a network of networks.

Most large communications companies have their own dedicated backbones connecting various regions. In each region, the company has a Point of Presence (POP). The POP is a place for local users to access the company's network, often through a local phone number or dedicated line. There are several high-level networks connecting to each other through Network Access Points or NAPs.

In the real Internet, dozens of large Internet Service Providers interconnect at NAPs in various cities, and trillions of bytes of data flow between the individual networks at these points. The Internet can be called a collection of huge corporate networks that agree to intercommunicate with each other at the NAPs. In this way, every computer on the Internet connects to every other. All of these networks rely on NAPs, backbones and routers to talk to each other. What is incredible about this process is that a message can leave one computer and travel halfway across the world through several different networks and arrive at another computer in a fraction of a second!

Internet Service Providers (ISPs)

An ISP is a company that provides individual users and businesses with connectivity to the Internet. Internet service providers (ISPs) also provide clients with access to Internet services such as Web hosting, Simple Mail Transfer Protocol (SMTP) mail, Usenet newsgroups, Internet Relay Chat (IRC), and downloadable Internet software.

ISPs come in various shapes and sizes, from volunteer-run freenets to local, regional, and national service providers such as BSNL. Many ISPs, still use freely available software such as Linux, Apache's Web server and sendmail for providing services to customers. Larger ISPs often use a heterogeneous network for providing core Web and mail services, as well as support for advanced Web and e-commerce applications for business and corporate clients.

Internet Backbones

The National Science Foundation (NSF) created the first high-speed backbone in 1987. Called NSFNET, it was a T1 line that connected 170 smaller networks together and operated at 1.544 Mbps (million bits per second). IBM, MCI and Merit worked with NSF to create the backbone and developed a T3 (45 Mbps) backbone the following year.

Backbones are typically fiber optic trunk lines. The trunk line has multiple fiber optic cables combined together to increase the capacity. Fiber optic cables are designated OC for optical carrier, such as OC-3, OC-12 or OC-48. An OC-3 line is capable of transmitting 155 Mbps while an OC-48 can transmit 2,488 Mbps (2.488 Gbps).

Today there are many companies that operate their own high-capacity backbones, and all of them interconnect at various NAPs around

the world. In this way, everyone on the Internet, no matter where they are and what company they use, is able to talk to everyone else on the planet. The entire Internet is a gigantic, sprawling agreement between companies to intercommunicate freely.

Clients and Servers

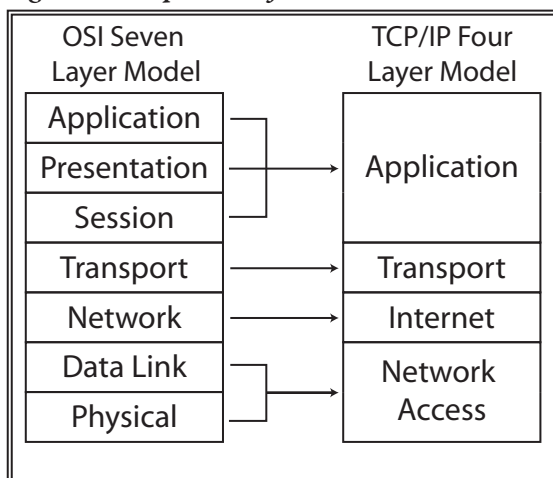
Internet servers make the Internet possible. All of the machines on the Internet are either servers or clients. The machines that provide services to other machines are servers. And the machines that are used to connect to those services are clients. There are Web servers, e-mail servers, FTP servers and so on serving the needs of Internet users all over the world.

When a client machine connects to a site to read a page, the server machine finds the page requested and sends it. Clients that come to a server machine do so with a specific intent, so clients direct their requests to a specific software server running on the server machine. For example, Web browser on the client machine will want to talk to the Web server software on the server machine and not to the e-mail server software.

TCP/IP

An abbreviation for Transmission Control Protocol/Internet Protocol, an industry-standard protocol suite for wide area networks (WANs) developed in the 1970s and 1980s by the U.S. Department of Defense (DoD). TCP/IP is a routable protocol that is suitable for connecting dissimilar systems (such as Microsoft Windows and UNIX) in heterogeneous networks, and it is the protocol of the Internet.

Figure 1: Comparison of OSI and TCP/IP



The architecture of the TCP/IP protocol suite has four layers that map loosely to the seven-layer Open Systems Interconnection (OSI) reference

model (as shown in the diagram). The TCP/IP model is sometimes called the DoD model because TCP/IP was developed in connection with the ARPANET project of the U.S. Department of Defense. Each layer of the TCP/IP protocol suite has its associated component protocols, the most important of which are listed here:

- ▶ **Application layer protocols:** Responsible for application-level access to TCP/IP networking services. These include Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet, Simple Mail Transfer Protocol (SMTP), and Simple Network Management Protocol (SNMP). In the Microsoft implementation of TCP/IP, application layer protocols interact with transport layer protocols by using either Windows Sockets or NetBIOS over TCP/IP (NetBT).
- ▶ **Transport layer protocols:** Establish communication through connection-oriented sessions and connectionless broadcasts. Protocols at this layer include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- ▶ **Internet layer protocols:** Responsible for routing and encapsulation into IP packets. Protocols at this layer include Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).
- ▶ **Network layer protocols:** Place frames on the network. These protocols include the various local area network (LAN) architectures (such as Ethernet and Token Ring) and WAN telecommunication service technologies—such as Plain Old Telephone Service (POTS), Integrated Services Digital Network (ISDN), and Asynchronous Transfer Mode (ATM).

The term host is most commonly used when discussing TCP/IP related services and functions. A host, in TCP/IP terms, is any network device that has a TCP/IP network address. Workstations, servers, and any other network device (as long as it has TCP/IP address) can all be considered hosts. TCP/IP uses two naming schemes to identify hosts and networks on an internetwork:

- ▶ **IP addresses:** Logical 32-bit numeric addresses of the form w.x.y.z. These are discussed in detail later in this chapter.
- ▶ **Fully qualified domain names (FQDNs):** Alphanumeric names of the form host_name.domain_name in which domain name is part of DNS, a hierarchical worldwide naming system. For example, the FQDN server12.microsoft.com represents a host named server12 that belongs to a network whose domain name is microsoft, which belongs to the top-level domain named .com, which belongs to the root DNS domain named dot. FQDNs are friendly names. They are easier to

Module 2, Chapter 4

remember than IP addresses and are resolved into IP addresses by using a DNS server or a local hosts file.

TCP/IP is a constantly evolving protocol suite whose development is steered by such bodies as the **INTERNET SOCIETY (ISOC)**, the **INTERNET ARCHITECTURE BOARD (IAB)**, and **THE INTERNET ENGINEERING TASK FORCE (IETF)**. The current version of TCP/IP is called IPv4 (Internet Protocol version 4); a new version called IPv6 is under development.

IP Addresses

Every machine on the Internet has a unique identifying number, called an IP Address. The IP stands for Internet Protocol. A server has a static IP address that does not change very often. A home machine that is dialing up through a modem, on the other hand, typically has an IP address assigned by the ISP every time it dials in. That IP address is unique for the session—it may be different the next time. This way, an ISP only needs one IP address for each modem it supports, rather than one for each customer.

A typical IP address looks like this:

216.27.61.137

IP addresses are normally expressed in decimal format as a dotted decimal number like the one above. But computers communicate in binary form.

The same IP address in binary would look as follows:

11011000.00011011.00111101.10001001

The four numbers in an IP address are called octets, because they each have eight positions when viewed in binary form. If all the positions are added together, the total is 32, which is why IP addresses are considered 32-bit numbers. Since each of the eight positions can have two different states (1 or zero), the total number of possible combinations per octet is 28 or 256. So each octet can contain any value between zero and 255. Combine the four octets for a total of 232 or a possible 4,294,967,296 unique values.

Out of the almost 4.3 billion possible combinations, certain values are restricted from use as typical IP addresses. For example, the IP address 0.0.0.0 is reserved for the default network and the address 255.255.255.255 is used for broadcasts.

The octets serve a purpose other than simply separating the numbers. They are used to create classes of IP addresses that can be assigned to a particular business, government or other entity based on size and need.

IP ADDRESS CLASS	POSSIBLE FIRST OCTET	USED FOR
Class A	1–126	Very large networks
Class B	128–191	Medium to large networks
Class C	192–223	Small networks
Class D	224–239	Multicasting
Class E	240–255	Reserved (experimental)

(IP addresses whose first octet is 127 represent the loop-back address and are used for troubleshooting purposes only, not for naming hosts.)

Domain Name Servers

Because most people have trouble remembering the strings of numbers that make up IP addresses, and because IP addresses sometimes need to change, all servers on the Internet also have easy-to-remember names, called domain names. For example, <http://www.yahoo.com> is a permanent, easy-to-remember name. It is easier for most to remember <http://www.yahoo.com> than it is to remember 66.218.71.90.

A set of servers called domain name servers (DNS) maps the easy-to-remember names to the IP addresses. These servers are simple databases that map alphabetic names to IP addresses, and they are distributed all over the Internet. Most individual companies, ISPs and universities maintain small name servers to map host names to IP addresses. There are also central name servers that use data supplied to map domain names to IP addresses.

Ports

Any server machine makes its services available to the Internet using numbered ports, one for each service that is available on the server. For example, if a server machine is running a Web server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21. Clients connect to a service at a specific IP address and on a specific port.

Each of the well-known services is available at a specific port number. Here are some common port numbers:

- ▶ echo 7
- ▶ daytime 13
- ▶ ftp 21
- ▶ telnet 23
- ▶ smtp 25 (Simple Mail Transfer Protocol, Outgoing e-mail)
- ▶ pop3 110 (Post Office Protocol [Version] 3, Incoming email)
- ▶ time 37
- ▶ nameserver 42
- ▶ WWW 80

Module 2, Chapter 4

If the server machine accepts connections on a port from the outside world, users can connect to the port from anywhere on the Internet and use the service.

Protocols

When a client has connected to a service on a particular port, it accesses the service using a specific protocol. The protocol is the pre-defined way that someone who wants to use a service talks with that service. The “someone” could be a person, but more often it is a computer program like a Web browser. Protocols are often in text format, and simply describe how the client and server will have their conversation.

Perhaps the simplest protocol is the **DAYTIME PROTOCOL**. If a user connects to port 13 on a machine that supports a daytime server, the server will send the current date and time and then close the connection. The protocol is, “If you connect to me, I will send you the date and time and then disconnect.”

Other popular services and protocols are E-mail (Simple Mail Transport Protocol or SMTP), Telnet (Telnet Protocol), and FTP (File Transfer Protocol) which will be discussed in the next section.

Internet Services

E-Mail

Electronic mail, or e-mail, allows computer users locally and worldwide to exchange messages. Each user of e-mail has a mailbox address to which messages are sent. Messages sent through e-mail can reach the destination within a matter of seconds.

A powerful aspect of e-mail is the option to send electronic files to a person’s e-mail address. Non-ASCII files, known as binary files, may be attached to e-mail messages. These files are referred to as MIME attachments. MIME stands for **MULTIMEDIA INTERNET MAIL EXTENSION**, and was developed to help e-mail software handle a variety of file types. For example, a document created in Microsoft Word can be attached to an e-mail message and retrieved by the recipient with the appropriate e-mail program. Many e-mail programs, including Eudora, Netscape Messenger, and Microsoft Outlook, offer the ability to read files written in HTML, which is itself a MIME type.

Telnet

Telnet is a program that allows users to log into computers on the Internet and use online databases, library catalogs, chat services, and more. There are no graphics in Telnet sessions, just text. To Telnet to a computer, users must know its address. This can consist of words (locis.loc.gov) or numbers (140.147.254.3). Some services require users to connect to a specific port on the remote computer. In this case, users have

to type the port number after the Internet address. Example: **TELNET nri.reston.va.us 185**

A link to a Telnet resource may look like any other link, but it will launch a Telnet session to make the connection. A Telnet program must be installed on the users local computer and configured to their Web browser in order to work.

With the increasing popularity of the Web, Telnet has become less frequently used as a means of access to information on the Internet.

FTP

FTP stands for File Transfer Protocol. This is both a program and the method used to transfer files between computers. Anonymous FTP is an option that allows users to transfer files from thousands of host computers on the Internet to their personal computer account. FTP sites contain books, articles, software, games, images, sounds, multimedia, course work, data sets, and more.

If a user's computer is directly connected to the Internet via an Ethernet cable, the user can use one of several PC software programs, such as WS_FTP for Windows, to conduct a file transfer.

FTP transfers can be performed on the World Wide Web without the need for special software. In this case, the Web browser will suffice. Whenever software is downloaded from a Web site to a user's local machine, FTP is being used. A user can also retrieve FTP files via search engines such as FtpFind. This option is easiest because the user does not need to know FTP program commands.

E-mail Discussion Groups

One of the benefits of the Internet is the opportunity it offers to people worldwide to communicate via e-mail. The Internet is home to a large community of individuals who carry out active discussions organized around topic-oriented forums distributed by e-mail. These discussions are administered by software programs. Probably the most commonly used program is the **LISTSERV**.

A great variety of topics are covered by listservs, many of them academic in nature. When a user subscribes to a listserv, messages from other subscribers are automatically sent to the user's electronic mailbox. A user can subscribe to a listserv by sending an e-mail message to a computer program called a listserver. Listservers are located on computer networks throughout the world. This program handles subscription information and distributes messages to and from subscribers. The user must have an e-mail account to participate in a listserv discussion group.

Module 2, Chapter 4

MAJORDOMO and **LISTPROC** are two other programs that administer e-mail discussion groups. The commands for subscribing to and managing list memberships are similar to those of **listserv**.

Usenet News

Usenet News is a global electronic bulletin board system in which millions of computer users exchange information on a vast range of topics. The major difference between Usenet News and e-mail discussion groups is the fact that Usenet messages are stored on central computers, and users must connect to these computers to read or download the messages posted to these groups. This is distinct from e-mail distribution, in which messages arrive in the electronic mailboxes of each list member.

Usenet itself is a set of machines that exchanges messages, or articles, from Usenet discussion forums, called newsgroups. Usenet administrators control their own sites, and decide which (if any) newsgroups to sponsor and which remote newsgroups to allow into the system.

There are thousands of Usenet newsgroups in existence. While many are academic in nature, numerous newsgroups are organized around recreational topics. Much serious computer-related work takes place in Usenet discussions. A small number of e-mail discussion groups also exist as Usenet newsgroups.

The Usenet newsfeed can be read by a variety of newsreader software programs. For example, the Netscape suite comes with a newsreader program called Messenger. Newsreaders are also available as standalone products.

FAQ, RFC, FYI

FAQ stands for **FREQUENTLY ASKED QUESTIONS**. These are periodic postings to Usenet newsgroups that contain a wealth of information related to the topic of the newsgroup. Many FAQs are quite extensive. FAQs are available by subscribing to individual Usenet newsgroups. A Web-based collection of FAQ resources has been collected by The Internet FAQ Consortium.

RFC stands for **REQUEST FOR COMMENTS**. These are documents created by and distributed to the Internet community to help define the nuts and bolts of the Internet. They contain both technical specifications and general information.

FYI stands for **FOR YOUR INFORMATION**. These notes are a subset of RFCs and contain information of interest to new Internet users.

Chat and Instant Messaging

Chat programs allow users on the Internet to communicate with each other by typing in real time. They are sometimes included as a feature of a Web site, where users can log into the “chat room” to exchange comments and information about the topics addressed on the site. Chat may take other, more wide-ranging forms. For example, America Online is well known for sponsoring a number of topical chat rooms.

INTERNET RELAY CHAT (IRC) is a service through which participants can communicate to each other on hundreds of channels. These channels are usually based on specific topics. While many topics are frivolous, substantive conversations are also taking place. To access IRC, users must use an IRC software program.

A variation of chat is the phenomenon of instant messaging. With instant messaging, a user on the Web can contact another user currently logged in and type a conversation. Popular instant messaging software are ICQ, MSN messenger and Google Talk.

World Wide Web

The most popular of Internet services, the World Wide Web, is rapidly changing the way business is done around the world. Most people consider the WWW and the Internet to be one and the same, whereas it is simply one of the many services provided by the Internet.

The World Wide Web is a system of Internet servers that supports hypertext to access several Internet protocols on a single interface. Almost every protocol type available on the Internet is accessible on the Web. This includes e-mail, Telnet, FTP, and Usenet News. In addition to these, the World Wide Web has its own protocol: Hyper Text Transfer Protocol, or HTTP. The working of the World Wide Web and these protocols will be explained in detail in the next section.

World Wide Web

The World Wide Web was developed in 1989 by **TIM BERNERS-LEE** of the European Particle Physics Lab (CERN) in Switzerland. The initial purpose of the Web was to use networked hypertext to facilitate communication among its members, who were located in several countries. Word was soon spread beyond CERN, and a rapid growth in the number of both developers and users ensued. In addition to hypertext, the Web began to incorporate graphics, video, and sound. The use of the Web has reached global proportions and has become a defining aspect of human culture in an amazingly short period of time.

Almost every protocol type available on the Internet is accessible on the Web. The following is a sample of major Internet protocols (discussed in the previous section) which are accessible on the Web:

Module 2, Chapter 4

E-mail (Simple Mail Transport Protocol or SMTP): Distributes electronic messages and files to one or more electronic mailboxes

Telnet (Telnet Protocol): Facilitates login to a computer host to execute commands.

FTP (File Transfer Protocol): Transfers text or binary files between an FTP server and client.

Usenet (Network News Transfer Protocol or NNTP): Distributes Usenet news articles derived from topical discussions on newsgroups.

HTTP (HyperText Transfer Protocol): Transmits hypertext over networks. This is the protocol of the Web.

The World Wide Web provides a single interface for accessing all these protocols. This creates a convenient and user-friendly environment. The Web gathers these protocols together into a single system. Because of this feature, and because of the Web's ability to work with multimedia and advanced programming languages, the Web is by far the most popular component of the Internet.

Hypertext and Links

The operation of the Web relies primarily on hypertext as its means of information retrieval. HyperText is a document containing words that connect to other documents. These words are called links and are selectable by the user. A single hypertext document can contain links to many documents. In the context of the Web, words or graphics may serve as links to other documents, images, video, and sound. Links may or may not follow a logical path, as each connection is created by the author of the source document. Overall, the Web contains a complex virtual web of connections among a vast number of documents, graphics, videos, and sounds.

Producing hypertext for the Web is accomplished by creating documents with a language called **HYPERTEXT MARKUP LANGUAGE** or HTML. With HTML, tags are placed within the text to accomplish document formatting, visual features such as font size, italics and bold, and the creation of hypertext links. Graphics may also be incorporated into an HTML document. HTML is an evolving language, with new tags being added with each upgrade. The **WORLD WIDE WEB CONSORTIUM (W3C)**, led by Tim Berners-Lee, coordinates the efforts of standardizing HTML. The W3C now calls the language XHTML and considers it to be an application of the XML language standard.

Web Pages

The World Wide Web consists of files, called pages or Web pages, containing information and links to resources throughout the Internet.

Web pages can be created by user activity. For example, when a user visits a Web search engine and enters keywords on the topic of their choice, a page will be created containing the results of their search. In fact, a growing amount of information found on the Web today is served from databases, creating temporary Web pages “on the fly” in response to user queries.

Access to Web pages may be accomplished by:

1. Entering an Internet address and retrieving a page directly
2. Browsing through pages and selecting links to move from one page to another
3. Searching through subject directories linked to organized collections of Web pages
4. Entering a search statement at a search engine to retrieve pages on the topic of choice

URL – Uniform Resource Locator

The URL specifies the Internet address of a file stored on a host computer connected to the Internet. Every file on the Internet, no matter what its access protocol, has a unique URL. Web browsers use the URL to retrieve the file from the host computer and the specific directory in which it resides. This file is then displayed on the monitor connected to the user’s local machine.

URLs are translated into numeric addresses using the Domain Name System (DNS). The DNS is a worldwide system of servers that stores location pointers to Web sites. The numeric address, called the IP (Internet Protocol) address, is actually the “real” URL. Since numeric strings are difficult for humans to use, alphanumeric addresses are employed by end users. Once the translation is made by the DNS, the browser can contact the Web server and ask for a specific file located on its site.

This is the format of the URL:

protocol://host/path/filename

For example, this is a URL on the Web site of the U.S. House of Representatives:

http://www.prime.com/common/about_us.html

Structure of this URL:

1. Protocol: **HTTP**
2. Host computer name: **WWW**
3. Second-level domain name: **PRIME**
4. Top-level domain name: **COM**
5. Directory name: **COMMON**
6. File name: **ABOUT_US.HTML**

Module 2, Chapter 4

It is easy to note how much information about the content of the file is present in this well-constructed URL.

The browser extracts the name “www.prime.com,” passes it to a domain name server, and the domain name server returns the correct IP address for www.prime.com. A number of name servers may be involved to get the right IP address.

Several top-level domains (TLDs) are common:

- com commercial enterprise
- edu educational institution
- gov U.S. government entity
- mil U.S. military entity
- net network access provider
- org usually nonprofit organizations

New domain names were approved in November 2000 by **THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)**: .biz, .museum, .info, .pro (for professionals) .name (for individuals), .aero (for the aerospace industry), and .coop (for cooperatives).

In addition, dozens of domain names have been assigned to identify and locate files stored on host computers in countries around the world. These are referred to as two-letter Internet country codes, and have been standardized by the International Standards Organization as ISO 3166.

For example:

- in India
- ch Switzerland
- de Germany
- jp Japan
- uk United Kingdom

As the technology of the Web evolves, URLs have become more complex. This is especially the case when content is retrieved from databases and served onto Web pages. The resulting URLs can have a variety of elaborate structures, for example,

<http://spills.incidentnews.gov/incidentnews/FMPro?-db=images&-Format=maps.htm&SpillLink=8&Subject=Waterway%20Closure%20Map&-SortField=EntryDate&-SortOrder=descend&-SortField=EntryTime&-SortOrder=descend&-Token=8&-Max=20&-Find>

The first part of this URL looks familiar. What follows are search elements that query the database and determine the order of the results. As a growing number of databases serve content to the Web, these types of URLs will appear more commonly in the browser’s address window.

Web Browsers

To access the World Wide Web, users must use a Web browser. A browser is a software program that allows users to access and navigate the World Wide Web. There are two types of browsers:

Graphical: Text, images, audio, and video are retrievable through a graphical software program such as Internet Explorer and Netscape. These browsers are available for Windows, Apple, Linux and other operating systems. Navigation is accomplished by pointing and clicking with a mouse on highlighted words and graphics.

Users can install a graphical browser such as Internet Explorer and Netscape in their computer. Internet Explorer is available on the Microsoft site: <http://www.microsoft.com/>. Netscape is available for downloading on the Netscape site: <http://home.netscape.com/>.

Other browsers are outside the mainstream but have their followers. Two examples are Opera and Firefox.

Text: Lynx is a browser that provides access to the Web in text-only mode. Navigation is accomplished by highlighting emphasized words in the screen with the arrow up and down keys, and then pressing the forward arrow (or Enter) key to follow the link. In these days of graphical browsers, it may be hard to believe that Lynx was once very popular.

Extending the Browser: Plug-Ins

Software programs may be configured to a Web browser in order to enhance its capabilities. When the browser encounters a sound, image or video file, it hands off the data to other programs, called plug-ins, to run or display the file. Working in conjunction with plug-ins, browsers can offer a seamless multimedia experience. Many plug-ins are available for free.

File formats requiring plug-ins are known as MIME types. MIME stands for Multimedia Internet Mail Extension, and was originally developed to help e-mail software handle a variety of binary (non-ASCII) file attachments. The use of MIME has expanded to the Web. For example, the basic MIME type handled by Web browsers is text/html associated with the file extension of html.

A common plug-in utilized on the Web is the Adobe Acrobat Reader. The Acrobat Reader allows users to view documents created in Adobe's Portable Document Format (PDF). These documents are the MIME type "application/pdf" and are associated with the file extension .pdf. When the Acrobat Reader has been configured to the user's browser, the program will open and display the file requested when the user clicks on a hyperlinked file name with the suffix .pdf. The latest versions of the

Module 2, Chapter 4

Acrobat Reader allow for the viewing of documents within the browser window.

Web browsers are often standardized with a small suite of plug-ins, especially for playing multimedia content. Additional plug-ins may be obtained at the browser's Web site, at special download sites on the Web, or from the Web sites of the companies that created the programs.

Once a plug-in is configured to the browser, it will automatically launch when the user chooses to access a file type that it uses.

Cookies

In Internet technologies, a cookie is a text file that a Web server saves on a client machine during a Hypertext Transfer Protocol (HTTP) session. Cookies are used to record information about the client's usage patterns, including the date and time the client visited the site, which pages were accessed, Web browser preferences, and so on. Cookies use the storage system of the client for saving this information instead of storing it on the server. Since the vast number of clients might visit the site only once, it would be inefficient to dedicate a large portion of server storage to tracking anonymous clients that might never return. Furthermore, client preferences (such as IP address) might change between sessions, especially for dial-up clients, so servers would have no way of recognizing clients if cookie information were saved on the server. Cookies therefore provide a way for the server to recognize that the client previously visited the site and record what the client did during previous visits, allowing the server to customize the HTTP session to meet the needs of the client.

Cookies are harmless text files and cannot be used to transmit a virus to the client. Cookies are simply passive holders of information; they cannot be used to "get" any information off the user's computer (such as e-mail address). Nevertheless, most Web browsers, such as Microsoft Internet Explorer, have an optional setting that allows users to reject cookies. However, rejecting cookies can result in poorer browsing experiences on sites that are cookie-dependent. Users can also delete any cookies on a computer running Microsoft Windows by deleting the contents of the cookies subdirectory within the user profile directory on their hard drive.

Active X

ActiveX is a technology developed by Microsoft which make plug-ins less necessary. ActiveX offers the opportunity to embed animated objects, data, and computer code on Web pages. A Web browser supporting ActiveX can render most items encountered on a Web page. For example, Active X allows users to view three-dimensional VRML (Virtual Reality Modelling Language) worlds in a Web browser without the use

of a VRML plug-in. As another example of the power of ActiveX, this technology can allow users to view and edit PowerPoint presentations directly within their Web browser. ActiveX works best with Microsoft's Internet Explorer.

Programming Languages and Functions

The use of existing and new programming languages have extended the capabilities of the Web. What follows is a basic guide to a group of the more common languages and functions in use on the Web today.

CGI

CGI (Common Gateway Interface) refers to a specification by which programs can communicate with a Web server. A CGI program, or script, is any program designed to accept and return data that conforms to the CGI specification. The program can be written in any programming language, including C, Perl, and Visual Basic Script. A common use for a CGI script is to process a form on a Web page. For example, users might fill out a form to order a book at a book site. The script processes the information and sends it to the web site to process the order.

ASP

Another type of dynamically generated Web page is called Active Server Pages (ASP). Developed by Microsoft, ASP is a programming environment that processes scripts on the Web server. The scripts run on the server, rather than on the Web browser, to generate the HTML pages sent to browsers. Visual Basic and JScript (a subset of JavaScript) are often used for the scripting. ASPs end in the file extension .asp or .aspx.

Java/Java Applets

Java is an object-oriented programming language similar to C++. Developed by Sun Microsystems, the aim of Java is to create programs that will be platform independent. The motto of Java is, "Write once, run anywhere." A perfect Java program should work equally well on a PC, Macintosh, Unix, and so on, without any additional programming. Java can be used to write applications for both Web and non-Web purpose.

Web-based Java applications are usually in the form of Java applets. These are small Java programs called from an HTML page that can be downloaded from a Web server and run on a Java-compatible Web browser. A few examples include live newsfeeds, moving images with sound, calculators, charts and spreadsheets, and interactive visual displays. Java applets can tend to load slowly, but programming improvements should lead to a shortened loading time.

JavaScript/Jscript

JavaScript is a programming language created by Netscape Communications. Small programs written in this language are embed-

Module 2, Chapter 4

ded within an HTML page, or called externally from the page, to enhance the functionality of the web page. Examples of JavaScript include moving tickers, drop-down menus, real-time calendars and clocks, and mouse-over interactions. Jscript is a similar language developed by Microsoft and works with the company's Internet Explorer browser.

VRML

VRML (Virtual Reality Modeling Language) allows for the creation of three-dimensional worlds. These may be linked from Web pages and displayed with a VRML viewer. One of the most interesting aspects of VRML is the option to "enter" the world and control movements within the world.

XML

XML (eXtensible Markup Language) is a mark-up language that enables Web designers to create their own customized tags to provide functionality not available with HTML. XML is a language of data structure and exchange and allows developers to separate form from content. With XML, the same content can be formatted for multiple applications. In May 1999, the W3 Consortium announced that HTML 4.0 has been recast as an XML application called XHTML. This move is having an impact on the future of both XML and HTML.

Intranets

A private TCP/IP internetwork within an organization that uses Internet technologies such as Web servers and Web browsers for sharing information and collaborating. Intranets can be used to publish company policies and newsletters, provide sales and marketing staff with product information, provide technical support and tutorials, and just about anything else that users want that fits within the standard Web server/Web browser environment.

Important Trends in the Web

Today's World Wide Web presents an ever-diversified experience of multimedia, programming languages, and real-time communication. There is no question that it is a challenge to keep up with the rapid pace of developments. The following presents a brief description of some of the more important trends to watch.

Multimedia

The Web has become a broadcast medium. It is possible to listen to audio and video over the Web, both pre-recorded and live. Several plug-ins are available for viewing these videos.

At one time, the entire multimedia file had to be downloaded before viewing. Since these types of files tend to be quite large, download times can be lengthy. This problem has been answered by a revolutionary de-

velopment in multimedia capability: **STREAMING MEDIA**. In this case, audio or video files are played as they are downloading, or streaming, into the user's computer. Only a small wait, called buffering, is necessary before the file begins to play.

The Windows Media Player, RealPlayer and QuickTime plug-ins play streaming audio and video files. Extensive files such as interviews, speeches and hearings work very well with these players. They are also ideal for the broadcast of real-time events. These may include live radio and television broadcasts, concerts, Web-only broadcasts, and so on.

SHOCKWAVE and **FLASH** are plug-ins that provide another multimedia experience. They offer the creation and implementation of an entire multimedia display combining graphics, animation and sound. Sound files, including music, are also a part of the Web experience. Sound files may be incorporated into Web sites, and are also available for downloading independent of Web site visits. For example, the search engine FindSounds.com can find sound files of different types. Sound files of many types are supported by the Web with the appropriate plug-ins. The MP3 file format, and the choice of supporting plug-ins, is one of the most popular music trends to sweep the Web.

Live cams are another aspect of the multimedia experience available on the Web. Live cams are video cameras that send their data in real time to a Web server. These cams may appear in all kinds of locations, both serious and whimsical: an office, on top of a building, a scenic locale, a special event, and so on.

Real-Time Communication

Text, audio and video communication can occur in real time on the Web. This capability allows people to conference and collaborate in real time. In general, the faster the Internet connection, the more successful the experience.

At its simplest, chat programs allow multiple users to communicate in text mode in real time. Internet Relay Chat and America Online's Instant Messenger are prime examples of this type of program. The development of open source messaging protocols like **JABBER** allows for the expansion of this capability throughout the Internet.

More enhanced real-time communication offers an audio and/or video component. CU-See Me is a popular software programs of this type. Even more elaborate are programs that allow for true real-time collaboration. Microsoft's NetMeeting and Netscape's Conference (available with Communicator) are good examples of this.

Collaboration tools include:

- ▶ audio: conduct a telephone conversation on the Web

Module 2, Chapter 4

- ▶ video: view the audience
- ▶ file transfer: send files back and forth among participants
- ▶ chat: type in real time
- ▶ whiteboard: draw, mark up, and save images on a shared window or board
- ▶ document/application sharing: view and use a program on another's desktop machine
- ▶ collaborative Web browsing: visit Web pages together

Currently no standard exists that will work among all conferencing programs.

Push

Push refers to a technology that sends data to a program without a request from the program. This is the opposite of the typical “pull” of the Web, in which the user clicks on a link to request a file from a server. With push, the data is sent automatically. Content is sent through a “channel.” The early Web-based implementation of push was commercial. Push can also be used to deliver software upgrades to desktop machines.

RSS

The abbreviation RSS can stand for different things, including Rich Site Summary or Really Simple Syndication. RSS allows people to place news and other announcement-like information into XML format that can then be pushed to RSS readers and Web pages. Users can subscribe to the RSS newsfeeds of their choice, and then have access to the updated information as it comes in. RSS is used for all kinds of purposes, including the news itself and announcing new content on Web sites.

RSS content may be read by using an RSS reader. This is software that posts new items and stores old ones in a graphical interface. An RSS reader is similar to e-mail software in that it displays incoming items and can store content for offline reading. Subscribing to a newsfeed is usually as simple as entering the URL of the RSS document.

Blogs

A blog is an easy-to-create Web site that allows users to share their thoughts with the world. The word “blog” comes from “Weblog” because a blog consists of a signed and dated log of individual postings.

Blogging is an interactive activity. Readers can add comments to a blogger's postings, other can respond, and a conversation ensues. Lately, bloggers have become well-known commentators on the political scene, but blogging can encompass any topic or no topic at all. Bloggers can use RSS to distribute their postings.

Summary

All of us are familiar with Internet. This chapter gives an intelligent appraisal of the whole gamut of technologies and services associated with Internet.

It starts with the why of Internet. From a historical perspective, the evolution of Internet is traced. Then who are all behind Internet - the organizations and service providers behind the Internet are explained.

Then the technologies that make this massive, ever growing network is explained. How is it that the communications occur without fail among the participants of this network? The addressing scheme is explained in this context.

The programming facilities available on the Internet are then explained.

What promises do the Internet hold for the future? This is an important question that needs to be addressed, considering the fact that Internet has changed many facets of public communication and commerce.

Next time, when you log on to Internet, you will have a different perspective of this mammoth network



5 Network Security

✂ Learning Goals ✂

This chapter deals with a variety of techniques associated with network security such as:

- Cryptography
- Security protocols
- Firewalls
- Intrusion Detection Systems
- Virtual Private Networks
- Penetration Testing
- Computer Forensics

Cryptography

Introduction

The word cryptography is derived from Greek and when literally translated, means “secret writing.” Before the advent of digital communications, cryptography was used primarily by the military. With the advances in modern communication, technology has enabled businesses and individuals to transport information at a very low cost through public networks such as the Internet. This development comes at the cost of potentially exposing the data transmitted over such a medium. Therefore, it becomes imperative for businesses to make sure that sensitive data is transferred from one point to another in a secure manner over public networks. Cryptography can help achieve this goal by making messages unintelligible to all but the intended recipient.

Encryption refers to the transformation of data from “plaintext” form into a form called “ciphertext,” which renders it almost impossible to read without the knowledge of a “key,” which can be used to reverse this transformation. The recovery of plaintext from the ciphertext requires the key, and this recovery process is known as decryption. This key is meant to be secret information and the privacy of the ciphertext depends on the cryptographic strength of the key.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called hackers or attackers.

Module 2, Chapter 5

Cryptography embraces both cryptography and cryptanalysis.

A related discipline is Steganography, which is the science of hiding messages rather than making them unreadable. Steganography is not cryptography. It relies on the secrecy of the mechanism used to hide the message. If, for example, a message is hidden in a graphic file, it is secret until someone knows to look for it, and then it provides no security at all.

Types of Cryptography

There are two types of cryptographic algorithms: Secret Key Cryptography and Public Key Cryptography.

Secret Key Cryptography

- ▶ This crypto-system uses the same key for both encryption and decryption (this is also referred to as “symmetric” cryptography).
- ▶ Both the sender and the receiver need to have the same key in order to communicate successfully.
- ▶ Examples: DES, 3-DES, RC4, RC5, etc.

Advantages:

- ▶ Very fast relative to public key cryptography;
- ▶ Depending on the algorithm and key, the encrypted message can be very secure;
- ▶ The ciphertext is compact (that is, encryption does not add much excess “baggage” to the ciphertext);
- ▶ Widely used and very popular.

Disadvantages:

- ▶ The administration of the keys can become extremely complicated;
- ▶ A large number of keys is needed to communicate securely with a large group of people;
- ▶ Non-repudiation is not possible
- ▶ The key is subject to interception by hackers.

Before 1970, this symmetric cryptographic system was the only system in existence. Before the advent of cheap computing power, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks. Public-key encryption is the technological revolution that provides strong cryptography to the masses.

Public Key Cryptography

- ▶ This crypto-system uses one key for encryption and another key for decryption (also known as “asymmetric” cryptography);
- ▶ Each user has two keys – one public key, which is revealed to all users, and one private key, which remains a secret. The private key and the public key are mathematically linked.

- Encryption is performed with the public key and decryption is performed with the private key or encryption is performed with the private key and decryption is performed with the public key
- Examples: RSA, Elgamal

Advantages:

- Considered very secure;
- No form of secret sharing is required, thus reducing key administration to a minimum;
- Supports non-repudiation;
- The number of keys managed by each user is much less compared to secret key cryptography.

Disadvantages:

- Much slower compared to secret key cryptography;
- The ciphertext is much larger than the plaintext, relative to secret key cryptography.

The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangement to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated. Some examples of public-key cryptosystems are Elgamal (named for its inventor, Taher Elgamal), RSA (named for its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman), Diffie-Hellman (named for its inventors), and DSA, the Digital Signature Algorithm, (invented by David Kravitz).

Basics of E-Security

Today's cryptography is more than just encryption and decryption. Cryptography is also closely tied to security. Public key cryptography, for instance, is heavily used for digital authentication purposes—i.e., assuring that communication is from a particular party. In today's digital world, authentication has become as important as privacy of data. In many cases, it is meaningless to encrypt data if the other party cannot be authenticated. Thus, strong authentication is becoming a necessity.

The following table highlights and defines the basic requirements for e-security.

LEVELS OF SECURITY	WHAT IS IT	HOW TO ACHIEVE
Authentication/ Verification	Establishes and verifies that the communicating parties are who they say they are.	Public key Cryptography
Confidentiality	Ensures the protection of sensitive and private data	Cryptography

LEVELS OF SECURITY	WHAT IS IT	HOW TO ACHIEVE
Data Integrity	Ensures that the data has not been altered or manipulated.	Encrypted Message Digests or Digital Signatures
Non-repudiation	Ensures that information cannot be disowned.	Digital Signatures authenticated by a CA

Digital Signatures

A major benefit of public key cryptography is that it provides a method for employing digital signatures. Digital signatures let the recipient of information verify the authenticity of the origin of the information and also verify that the information was not altered while in transit. Thus, public key digital signatures provide authentication and data integrity. These features are every bit as fundamental to cryptography as confidentiality, if not more.

A digital signature serves the same purpose as a seal on a document, or a handwritten signature. However, because of the way it is created, it is superior to a seal or signature in an important way. A digital signature not only attests to the identity of the signer, but it also shows that the contents of the information signed have not been modified. A physical seal or handwritten signature cannot do that. However, like a physical seal that can be created by anyone with possession of the signet, a digital signature can be created by anyone with the private key of that signing key-pair.

While it is possible for the public key algorithm to encrypt the message using the sender’s private key and have the receiver use the public key to verify it. This is usually not done for two reasons. First, encrypting a message using public key is very slow. Secondly, in most instances, authentication and integrity is important by secrecy is not required. It many case, when a message is sent to several recipients it may be necessary for many people who do not have the private key to view the message even though they cannot authenticate it.

Hash functions

An improvement on the above scheme is the addition of a one-way hash function in the process. A one-way hash function takes variable-length input—in this case, a message of any length, even thousands or millions of bits—and produces a fixed-length output; say, 160 bits. The hash function ensures that, if the information is changed in any way—even by just one bit—an entirely different output value is produced.

For example, PGP (Pretty Good Privacy) software uses a cryptographically strong hash function on the plaintext. This generates a fixed-length data item known as a message digest. (Any change to the plaintext results in a totally different digest.)

Then PGP uses the digest and the private key to create the “signature”. PGP transmits the signature and the plaintext together. Upon receipt of the message, the recipient uses PGP to re-compute the digest and verify the signature. PGP can at the sender’s option, encrypt and sign the message; signing plaintext is useful if some of the recipients are not interested in or capable of verifying the signature.

Digital Signature Certificates

One issue with public key cryptosystems is that users must be constantly vigilant to make sure they are encrypting to the correct person’s key. In an environment where it is safe to freely exchange keys through public servers, man-in-the-middle attacks are a potential threat. In this type of attack, someone posts a phony key with the name and user ID of the user’s intended recipient. Data encrypted to—and intercepted by—the true owner of this bogus key is now in the wrong hands.

In a public key environment, it is vital that users know for certain that the public key with which they are encrypting data is in fact the public key of the intended recipient, and not a forgery. They could simply encrypt only to those keys that have been physically handed to them. But suppose they need to exchange information with people they have never met; how can they be sure they have the correct key?

Digital signature certificates simplify the task of establishing whether a public key truly belongs to the purported owner. A certificate is a form of credential. Other kinds of credentials include driver’s license, social security card, and birth certificate. Each of these has some information on it identifying the user and some authorization stating that someone else has confirmed their identity. Some certificates, such as a passport, are important enough confirmation of a user’s identity that they would not want to lose them, lest someone else use the passport to impersonate the real owner.

A digital signature certificate functions much like a physical certificate. A digital signature certificate contains a person’s public key that helps others verify that a key is genuine or valid. Digital certificates are used to thwart attempts to substitute one person’s key for another.

A digital signature certificate consists of four things:

- ▶ A public key
- ▶ Certificate information (usually “identity” information about the user, such as name, user ID and so on. Certificates may also contain

Module 2, Chapter 5

authorization information about the user, such as spending limit, file permissions, and so on.)

- ▶ One or more digital signatures of the trusted organization
- ▶ Validity period

The purpose of the digital signature on a certificate is to state that the certificate information has been attested by a trusted third party. Thus, a certificate is basically a public key with one or two forms of ID attached, plus a stamp of approval from some trusted organization.

Certificate distribution

Certificates are used when it is necessary to exchange public keys with someone else. For small groups of people who wish to communicate securely, it is easy to manually exchange diskettes or emails containing each owner's public key.

For larger groups, it is necessary to put systems into place that can provide the necessary security, storage, and exchange mechanisms so that coworkers, business partners, or strangers could communicate with a particular individual. This purpose is served by storage-only repositories called Certificate Servers, or more structured systems that provide additional key management features and are called Public Key Infrastructures (PKIs).

Certificate servers

A certificate server is a network-available database that allows users to submit and receive digital certificates. Often, certificate servers are also general-purpose directory servers. A certificate server may also provide some administrative features that help a company maintain its security policies. An example might be allowing only the storage of keys that meet certain requirements. The PGP Keyserver (formerly known as the PGP Certificate Server) provides these, whereas generic directory servers may not.

Public Key Infrastructures (PKIs)

A PKI includes the certificate storage facilities of a certificate server, but also provides services and protocols for managing public keys. These include the ability to issue, revoke, and trust certificates. The main feature of a PKI is the introduction of what are known as **CERTIFICATION AUTHORITY (CA)** and **REGISTRATION AUTHORITY (RA)** components.

A CA creates certificates and digitally signs them using the CA's private key. Because of its role in creating certificates, the CA is the central component of a PKI. Using the CA's public key, anyone wanting to verify a certificate's authenticity verifies the issuing CA's digital signature, and

hence, the integrity of the contents of the certificate (most importantly, the public key and the identity of the certificate holder).

Typically, a RA refers to the people, processes, and tools used to support the registration of users with the CA (enrollment) and ongoing administration of users. The RA may perform vetting—the process of verifying that a public key belongs to its purported owner.

Certificate Format

A digital certificate is basically a collection of identifying information bound together with a public key and signed by a trusted third party to prove its authenticity. A digital certificate can be one of a number of different formats.

X.509 is the most commonly used certificate format. All X.509 certificates comply with the ITU-T X.509 international standard; thus (theoretically) X.509 certificates created for one application can be used by any application complying with X.509. In practice, however, different companies have created their own extensions to X.509 certificates, not all of which work together.

A certificate requires someone to validate that a public key and the name of the key's owner go together. With X.509 certificates, the validator is always a Certification Authority or someone designated by a CA.

An X.509 certificate is a collection of a standard set of fields containing information about a user or device and their corresponding public key. The X.509 standard defines what information goes into the certificate, and describes how to encode it (the data format).

All X.509 certificates have the following data:

- ▶ The certificate holder's public key—the public key of the certificate holder, together with an algorithm identifier that specifies which cryptosystem the key belongs to and any associated key parameters.
- ▶ The serial number of the certificate—the entity (application or person) that created the certificate is responsible for assigning it a unique serial number to distinguish it from other certificates it issues. This information is used in numerous ways; for example when a certificate is revoked, its serial number is placed on a Certificate Revocation List (CRL).
- ▶ The certificate holder's unique identifier (or DN—distinguished name)—this name is intended to be unique across the Internet. A DN consists of multiple subsections and may look something like this:

CN=Bob Davis, EMAIL=bdavis@agp.com, OU=AGP Engineering, O=AGP Corporation, C=US
(These refer to the subject's Common Name, Organizational Unit, Organization, and Country.)

Module 2, Chapter 5

- ▶ The certificate's validity period—the certificate's start date/time and expiration date/time; indicates when the certificate will expire.
- ▶ The unique name of the certificate issuer - the unique name of the entity that signed the certificate. This is normally a CA. Using the certificate implies trusting the entity that signed this certificate. (Note that in some cases, such as root or top-level CA certificates, the issuer signs its own certificate.)
- ▶ The digital signature of the issuer—the signature using the private key of the entity that issued the certificate.
- ▶ The signature algorithm identifier—identifies the algorithm used by the CA to sign the certificate.
- ▶ To obtain an X.509 certificate, the user must ask a CA to issue one. The user provides his public key, proof that he possesses the corresponding private key, and some specific information about himself. He then digitally signs the information and sends the whole package—the certificate request—to the CA. The CA then performs some due diligence in verifying that the information he provided is correct and, if so, generates the certificate and returns it.

Security Protocols

SSL

The SSL (Secure Sockets Layer) Protocol was developed by Netscape Communications Corporation to provide security and privacy over the Internet. The protocol supports server and client authentication. The SSL protocol is application independent, allowing protocols like HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), and Telnet to be layered on top of it transparently. The SSL protocol is able to negotiate encryption keys as well as authenticate the server before data is exchanged by the higher-level application. The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a protocol that adds digital signatures and encryption to Internet MIME (Multipurpose Internet Mail Extensions) messages. MIME is the standard format for extended Internet electronic mail. Internet e-mail messages consist of two parts, the header and the body. The header forms a collection of field/value pairs structured to provide information essential for the transmission of the message. The body is normally unstructured unless the e-mail is in MIME format. MIME defines how the body of an e-mail message is structured. The MIME format permits e-mail to include enhanced text, graphics, audio, and more in a standardized manner via MIME-compliant mail systems. However, MIME itself does not provide any security services. The purpose of S/MIME is to define such services, following the syntax for digital signatures and encryption.

IPSec

The Internet Engineering Task Force (IETF)'s IP Security Protocol (IPSec) working group is defining a set of specifications for cryptography-based authentication, integrity, and confidentiality services at the IP datagram layer. IPSec is intended to be the future standard for secure communications on the Internet, but is already the de facto standard. The IPSec group's results comprise a basis for interoperably secured host-to-host pipes, encapsulated tunnels, and Virtual Private Networks (VPNs), thus providing protection for client protocols residing above the IP layer.

The protocol formats for IPSec's Authentication Header (AH) and IP Encapsulating Security Payload (ESP) are independent of the cryptographic algorithm, although certain algorithm sets are specified as mandatory for support in the interest of interoperability. Similarly, multiple algorithms are supported for key management purposes (establishing session keys for traffic protection), within IPSec's framework.

SSH

SSH, or Secure Shell, is a protocol which permits secure remote access over a network from one computer to another. SSH negotiates and establishes an encrypted connection between a SSH client and a SSH server, authenticating the client and server in any of a variety of ways (some of the possibilities for authentication are RSA, SecurID, and passwords). That connection can then be used for a variety of purposes, such as creating a secure remote login on the server (effectively replacing commands such as telnet, rlogin, and rsh) or setting up a VPN (Virtual Private Network).

Kerberos

Kerberos is an authentication service developed by the Project Athena team at MIT. Unlike a public-key authentication system, Kerberos does not produce digital signatures. Instead Kerberos was designed to authenticate requests for network resources rather than to authenticate authorship of documents. Thus, Kerberos does not provide for future third-party verification of documents.

In a Kerberos system, there is a designated site on each network, called the Kerberos server, which performs centralized key management and administrative functions. The server maintains a database containing the secret keys of all users, authenticates the identities of users, and distributes session keys to users and servers who wish to authenticate one another. Kerberos requires trust in a third party (the Kerberos server). If the server is compromised, the integrity of the whole system is lost. Public-key cryptography was designed precisely to avoid the necessity to trust third parties with secrets. Kerberos is generally considered ad-

Module 2, Chapter 5

equate within an administrative domain; however across domains the more robust functions and properties of public-key systems are often preferred. There has been some developmental work in incorporating public-key cryptography into Kerberos.

SET

Visa and MasterCard have jointly developed the Secure Electronic Transaction (SET) protocol as a method for secure, cost effective bank-card transactions over open networks. SET includes protocols for purchasing goods and services electronically, requesting authorization of payment, and requesting “credentials” (that is, certificates) binding public keys to identities, among other services. Once SET is fully adopted, the necessary confidence in secure electronic transactions will be in place, allowing merchants and customers to partake in electronic commerce.

Firewalls

Introduction

Network firewalls are devices or systems that control the flow of network traffic between networks employing differing security postures. In most modern applications, firewalls and firewall environments are discussed in the context of Internet connectivity and the TCP/IP protocol suite. However, firewalls have applicability in network environments that do not include or require Internet connectivity. For example, many corporate enterprise networks employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel department. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas. The inclusion of a proper firewall or firewall environment can therefore provide an additional layer of security that would not otherwise be available.

Basic firewalls will operate on a smaller number of layers of the OSI model; more advanced firewalls will cover a larger number of layers. In terms of functionality, firewalls capable of examining a larger number of layers are more thorough and effective. Additional layer coverage also increases the configuration granularity present in the firewall; adding layer awareness allows the firewall to accommodate advanced applications and protocols. Increasing the layers a firewall can examine also allows the firewall to provide services that are highly user-oriented, such as user authentication. A firewall that function with layers 2 and 3 only does not usually deal with specific users, but a higher end application-proxy gateway firewall can enforce user authentication as well as logging events to specific users.

Firewalls can also act as Virtual Private Network (VPN) gateways. Thus, an organization or agency can send unencrypted network traffic from systems behind the firewall to other remote systems behind a cooperating VPN gateway; the firewall encrypts the traffic and forwards it to the remote VPN gateway, which decrypts it and passes it on to the destination systems. Most of the more popular firewalls nowadays incorporate this type of functionality (VPNs are discussed in greater detail in later section).

The final add-on involves active content filtering technologies. This mechanism differs from the normal function of a firewall in that the firewall can also be capable of filtering the actual application data at layer 7 that seeks to traverse the firewall. For example, this mechanism might be employed to scan email attachments and remove viruses. It is also widely used to filter the more dangerous active web-enabling technologies, such as Java.3, JavaScript, and ActiveX. Or, it can be used to filter on contents or keywords to restrict web access to inappropriate sites or domains. However, firewall-based content filtering should not be relied upon as the sole content filtering mechanism for an organization or agency; it is possible to bypass these filters through the use of compression or encryption or other techniques.

Packet Filter Firewalls

The most basic, fundamental type of firewall is called a packet filter. Packet filter firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions. The access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a ruleset.

In their most basic form, packet filters operate at Layer 3 or Network layer of the OSI model. This basic functionality is designed to provide network access control based upon several pieces of information contained in a network packet:

- ▶ The **SOURCE ADDRESS** of the packet, i.e., the Layer 3 address of the computer system or device the network packet originated from (an IP address such as 192.168.1.1).
- ▶ The **DESTINATION ADDRESS** of the packet, i.e., the Layer 3 address of the computer system or device the network packet is trying to reach (e.g., 192.168.1.2).
- ▶ The **TYPE OF TRAFFIC**, that is, the specific network protocol being used to communicate between the source and destination systems or devices
- ▶ Possibly some characteristics of the Layer 4 communications sessions, such as the **SOURCE AND DESTINATION PORTS** of the sessions (e.g., TCP:80 for the destination port belonging to a web server,

Module 2, Chapter 5

TCP:1320 for the source port belonging to a personal computer accessing the server).

- ▶ Sometimes, information pertaining to **WHICH INTERFACE OF THE ROUTER THE PACKET CAME FROM** and which interface of the router the packet is destined for; this is useful for routers with 3 or more network interfaces.

Advantages of Packet Filter Firewalls

- ▶ Packet filter firewalls have two main strengths: speed and flexibility. Since packet filters do not usually examine data above Layer 3 of the OSI model, they can operate very quickly. Likewise, since most modern network protocols can be accommodated using Layer 3 and below, packet filter firewalls can be used to secure nearly any type of network communication or protocol. This simplicity allows packet filter firewalls to be deployed into nearly any enterprise network infrastructure.
- ▶ An important point is that their speed and flexibility, as well as capability to block denial-of-service and related attacks, makes them ideal for placement at the outermost boundary with an untrusted network. The packet filter, referred to as a **BOUNDARY ROUTER**, can block certain attacks, possibly filter unwanted protocols, perform simple access control, and then pass the traffic onto other firewalls that examine higher layers of the OSI stack.

Disadvantages of Packet Filter Firewalls

Packet filter firewalls also possess several weaknesses:

- ▶ Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions. For example, a packet filter firewall cannot block specific application commands; if a packet filter firewall allows a given application, all functions available within that application will be permitted.
- ▶ Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).
- ▶ Most packet filter firewalls do not support advanced user authentication schemes. Once again, this limitation is mostly due to the lack of upper-layer functionality by the firewall.
- ▶ They are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing. Many packet filter firewalls cannot detect a network packet in which the OSI Layer 3 addressing information has been altered. Spoofing attacks are generally em-

ployed by intruders to bypass the security controls implemented in a firewall platform.

- ▶ Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations. In other words, it is easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based upon an organization's information security policy.

Consequently, packet filter firewalls are very suitable for high-speed environments where logging and user authentication with network resources is not important. Since current firewall technology includes many features and functionality, it is difficult to identify a single firewall that contains only packet filter features. The closest example would be a network router employing coded access control lists to handle network traffic. Most SOHO (Small Office Home Office) firewall appliances and default operating system firewalls are packet filter firewalls.

Application-Proxy Gateway Firewalls

Application-Proxy Gateway firewalls are advanced firewalls that combine lower layer access control with upper layer (Layer 7 or Application Layer) functionality.

Application-proxy gateway firewalls do not require a Layer 3 (Network Layer) route between the inside and outside interfaces of the firewall; the firewall software performs the routing. In the event the application-proxy gateway software ceases to function, the firewall system is unable to pass network packets through the firewall system. All network packets that traverse the firewall must do so under software (application-proxy) control.

Each individual application-proxy, also referred to as a proxy agent, interfaces directly with the firewall access control ruleset to determine whether a given piece of network traffic should be permitted to transit the firewall. In addition to the ruleset, each proxy agent has the ability to require authentication of each individual network user. This user authentication can take many forms, including the following:

- ▶ User ID and Password Authentication,
- ▶ Hardware or Software Token Authentication,
- ▶ Source Address Authentication, and
- ▶ Biometric Authentication

Advantages

Application-proxy gateway firewalls have numerous advantages over packet filter firewalls and stateful inspection packet filter firewalls.

- ▶ First, application-proxy gateway firewalls usually have more extensive logging capabilities due to the firewall being able to examine the

Module 2, Chapter 5

entire network packet rather than just the network addresses and ports. For example, application-proxy gateway logs can contain application-specific commands within the network traffic.

- ▶ Another advantage is that application-proxy gateway firewalls allow security administrators to enforce whatever type of user authentication is deemed appropriate for a given enterprise infrastructure. Application-proxy gateways are capable of authenticating users directly, as opposed to packet filter firewalls and stateful inspection packet filter firewalls that normally authenticate users based on the network layer address of the system they reside on. Given that network layer addresses can be easily spoofed, the authentication capabilities inherent in application-proxy gateway architecture are superior to those found in packet filter or stateful inspection packet filter firewalls.
- ▶ Finally, given that application-proxy gateway firewalls are not simply Layer 3 devices, they can be made less vulnerable to address spoofing attacks.

Disadvantages

The advanced functionality of application-proxy gateway firewalls also fosters several disadvantages when compared to packet filter or stateful inspection packet filter firewalls.

- ▶ First, because of the full packet awareness found in application-proxy gateways, the firewall is forced to spend quite a bit of time reading and interpreting each packet. For this reason, application-proxy gateway firewalls are not generally well suited to high-bandwidth or real-time applications. To reduce the load on the firewall, a dedicated proxy server can be used to secure less time-sensitive services such as email and most web traffic.
- ▶ Another disadvantage is that application-proxy gateway firewalls tend to be limited in terms of support for new network applications and protocols. An individual, application-specific proxy agent is required for each type of network traffic that needs to transit a firewall. Most application-proxy gateway firewall vendors provide generic proxy agents to support undefined network protocols or applications. However, those generic agents tend to negate many of the strengths of the application-proxy gateway architecture and they simply allow traffic to tunnel through the firewall.

Dedicated Proxy Servers

Dedicated proxy servers differ from application-proxy gateway firewalls in that they retain proxy control of traffic but they do not contain firewall capability. They are typically deployed behind traditional firewall platforms for this reason. In typical use, a main firewall might accept inbound traffic, determine which application is being targeted and then

hand off the traffic to the appropriate proxy server, e.g., an email proxy server. The proxy server typically would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery. An example of this would be an HTTP proxy deployed behind the firewall; users would need to connect to this proxy en route to connecting to external web servers. Typically, dedicated proxy servers are used to decrease the work load on the firewall and to perform more specialized filtering and logging that otherwise might be difficult to perform on the firewall itself.

As with application-proxy gateway firewalls, dedicated proxies allow an organization to enforce user authentication requirements as well as other filtering and logging on any traffic that traverses the proxy server. The implications are that an organization can restrict outbound traffic to certain locations or could examine all outbound email for viruses or restrict internal users from writing to the organization's web server. Security experts have stated that most security problems occur from within an organization; proxy servers can assist in foiling internally based attacks or malicious behavior. At the same time, filtering outbound traffic will place a heavier load on the firewall and increase administration costs.

In addition to authentication and logging functionality, dedicated proxy servers are useful for web and email content scanning, including the following:

- ▶ Java applet or application filtering (signed versus unsigned or universal)
- ▶ ActiveX control filtering (signed versus unsigned or universal)
- ▶ JavaScript filtering
- ▶ Blocking specific Multipurpose Internet Multimedia Extensions (MIME) types. For example, Microsoft Word documents
- ▶ Virus scanning and removal
- ▶ Macro virus scanning, filtering, and removal
- ▶ Application-specific commands, for example, blocking the HTTP delete command, and
- ▶ User-specific controls, including blocking certain content types for certain users.

Hybrid Firewall Technologies

Recent advances in network infrastructure engineering and information security have caused a blurring of the lines that differentiate the various firewall platforms discussed earlier. As a result of these advances, firewall products currently incorporate functionality from several different classifications of firewall platforms. For example, many Application-

Module 2, Chapter 5

Proxy Gateway firewall vendors have implemented basic packet filter functionality in order to provide better support.

Likewise, many packet filter or stateful inspection packet filter firewall vendors have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or stateful inspection packet filter firewall vendors implement application proxies to provide improved network traffic logging and user authentication in their firewalls.

Nearly all major firewall vendors have introduced hybridization into their products in some way, shape or form, so it is not always a simple matter to decide which specific firewall product is the most suitable for a given application or enterprise infrastructure. Hybridization of firewall platforms makes the pre-purchase product evaluation phase of a firewall project important. Supported feature sets, rather than firewall product classification, should drive the product selection.

Host-Based firewalls

Firewall packages are available in some operating systems such as Linux or as add-ons where they can be used to secure the individual host only. This can be helpful for use with internal servers; for example, an internal web server could be placed on a system running a host-based firewall. This carries several advantages, including the following:

- ▶ The server application is protected better than if it were running alone; internal servers should be protected and should not be assumed to be safe from attack because they are behind a main firewall.
- ▶ A separate firewall and subnet are not necessary for securing the server; the host-based firewall performs these functions.

Host-based firewall packages typically provide access-control capability for restricting traffic to and from servers running on the host, and there is usually some limited logging available. While a host-based firewall is less desirable for high-traffic, high-security environments, in internal network environments or regional offices they offer greater security usually at a lower cost. A disadvantage to host-based firewalls is that they must be administered separately, and after a certain number it becomes easier and less expensive to simply place all servers behind a dedicated firewall configuration.

Personal Firewalls/Personal Firewall Appliances

Securing personal computers at home or remote locations is now as important as securing them at the office; many people telecommute or work at home and operate on organization- or agency-proprietary data. Home users dialing an Internet Service Provider (ISP), may have little firewall protections available to them because the ISP has to accom-

moderate potentially many different security policies. Therefore, personal firewalls have been developed to provide protection for remote systems and to perform many of the same functions as larger firewalls.

These products are typically implemented in one of two configurations. One of these configurations is a **PERSONAL FIREWALL**, which is installed on the system it is meant to protect; personal firewalls usually do not offer protection to other systems or resources. Likewise, personal firewalls do not typically provide controls over network traffic that is traversing a computer system. They only protect the computer system they are installed on.

The second configuration is called a **PERSONAL FIREWALL APPLIANCE**, which is in concept more similar to that of a traditional firewall. In most cases, personal firewall appliances are designed to protect small networks such as networks that might be found in home offices. These appliances usually run on specialized hardware and integrate some other form of network infrastructure components in addition to the firewall itself, including the following:

- ▶ Cable Modem WAN Routing
- ▶ LAN Routing (dynamic routing support)
- ▶ Network hub
- ▶ Network switch
- ▶ DHCP (Dynamic Host Configuration Protocol) server
- ▶ Network management (SNMP) agent
- ▶ Application-proxy agents

Incorporating these infrastructure components into a firewall appliance allows an organization to deploy effective solutions consisting of a single piece of hardware.

Demilitarized Zone (DMZ)

In the context of firewalls, DMZ refers to a part of the network that is neither part of the internal network nor directly part of the Internet. Typically, this is the area between the Internet access router and the bastion host, though it can be between any two policy-enforcing components of the architecture.

A DMZ can be created by putting access control lists on the access router. This minimizes the exposure of hosts on the external LAN by allowing only recognized and managed services on those hosts to be accessible by hosts on the Internet. Many commercial firewalls simply make a third interface off of the bastion host and label it the DMZ. The point is that the network is neither “inside” nor “outside”.

Intrusion Detection Systems (IDS)

Introduction

If one wishes to compare information security to a home anti-burglary system, firewalls perform the role of door and window locks. These types of locks will stop the majority of burglars but sophisticated intruders may circumvent security devices that protect an intended target i.e. a home. Therefore, people use a combination of sophisticated locks with alarm systems. An IDS performs the role of such an alarm system and adds the next preventive layer of security by detecting attacks that penetrate IT systems.

IDS originators assumed that no protection system could make a network 100 percent secure against outside attacks. Once the protection barrier has been negotiated, such an anomalous situation must be reported to the system administrator as quickly as possible. It would be useful to view what an intruder was doing in an IT system. These are the key tasks for Intrusion Detection System programs. For more details on the function of an IDS, please refer to the next module.

IDS operation

IDS performs a continuous monitoring of events. The intrusion detection software monitors the server and logs any unauthorized access attempts and aberrant behavior patterns. Of course, an IDS must be instructed to recognize such events. IDS can process various types of data, such as, traffic eavesdropping, packets flowing into system logs, information on user's activities. In operational terms, three primary types of intrusion detection systems are available:

- ▶ Host-based systems - HIDS,
- ▶ Network-based systems - NIDS,
- ▶ Network node-based systems - NNIDS.

Host-based IDS (HIDS)

This is a software that is based on auditing whatever information it can glean as generated by the OS activities. Such information can include system-generated logs, system events (e.g. unauthorized login attempts, aberrant file accesses, file status etc.). Generally an IDS deals with all IT systems that can be monitored.

Network-based IDS (NIDS)

The software belonging to this IDS group analyzes network packets. An NIDS agent places the network interface card into "promiscuous" mode and audits all traffic crossing the interface. As a general rule, it should be able to analyse all traffic within a specific network segment. Therefore, with switched networks, an NIDS agent should be connected to the monitoring port of the hub. An NIDS agent functions as an appropriate software module that resides on one of the servers within a

LAN segment. However, one must remember that the volume of packets sent over contemporary LANs is enormous. And this volume must be analyzed by an NIDS. If the agent has inadequate capacity to handle extreme loads, it can miss packets due to congestion on the network link that it is monitoring and fail to collect the next packets that are received. Therefore, functioning under a regime close to the real-time mode is a must for an NIDS.

On the other hand, an NIDS agent itself may overload the system it resides in and “incapacitate” the system to perform other tasks. This weakness spurs NIDS manufacturers to develop data collecting agents as a dedicated system to be installed on a separate robust PC (for instance, NFR NID-100 is offered as a CD-ROM to boot the system). Another option is a complete system encompassing both hardware and software (for example, Cisco NetRanger is a Cisco software-based PC running on Solaris operating system).

NIDS are installed per network segment coverage associated with characteristic attacks (for example, ping of death) or else used to deal with lesser events that are not simply attacks but preparative steps (for example, port scan).

Network Node IDS (NNIDS)

This IDS sub-approach is a specific modification of NIDS. Traditional NIDS agents, with the network interface set properly, collect data intended for the whole network. On the other hand, NNIDS are composed of micro agents distributed over each workstation within a network segment. Each micro agent monitors the network traffic directed to that workstation only, greatly reducing the capacity requirements needed by the NIDS. The weaknesses of NNIDS are associated with the requirement to have and manage a huge amount of micro agents as well as with the fact that NNIDS may have difficulty detecting attacks for which the coverage of the entire network is required, for example, to detect TCP Stealth Scanning. Such a traffic analysis approach is a must in VPNs, when the end-to-end encryption technique is employed. No traditional NIDS will be able to audit such traffic, as it is encrypted. A NNIDS analyses instantly, after decryption is made.

Selection of an IDS

Security administrators or integrators wishing to install IDS, must take into consideration that this is a serious task. Therefore, it is critical to understand the properties of IDS technologies and the working environment to be used and also to have a broad knowledge of contemporary intrusion types. Contrary to firewall solutions, with IDS a more rigorous configuration policy is necessary, as they are much more sophisticated tools. Therefore, it is a good idea to outsource the implementing of an IDS service to specialists.

IDS Modules

Basically, the current generation of IDS programs has a modular architecture. In its most basic form, IDS architecture consists of the following modules:

- ▶ **IDS agents** that collect information: These are software programs that reside on servers (HIDS) within critical network segments (NIDS), or on each network node (NNIDS). Agents are key issues for IDS functioning. They may generate alerts for malicious activities.
- ▶ **Database:** Here, all data collected by agents are stored. By auditing data gathered by all agents, certain attacks that are threats for the entire network can be detected and also trends and patterns of attack on the network may be tracked.
- ▶ **Manager:** This is a console that manages all modules. The manager is the administrator's interface.
- ▶ **Alert Generator:** This module is responsible for notifying the administrator about a potential threat. Currently, a variety of IDS approaches are available. Certain IDS are limited to generate alerts (which may be logged) or others which may be placed on the management console only (Snort, Cisco RealSecure) and are based on outside software for information processing purposes (Cisco recommends, for example, netForensics). Other solutions can take the form of a wide range of sophisticated notifications (e-mail, SNMP trap, displaying a console box, fax, SMS, sending messages to the managing software, launching any deliberate program).
- ▶ **Report Generator:** This is a software module designed to generate reports based on the collected data.

When fitting an IDS within the rest of the security framework, protection of inside communication is to be considered with proper care. If the inter-module transmission is prone to sniffing and eavesdropping, the IDS itself will be vulnerable to attacks. Inter-module communications should be encrypted using all well recognized security standards. Ad hoc encryption standards produced by early adopters or non-published standards should be avoided. Secure and trusted IDS employ IPSec technology to encrypt packets. If a specific IDS is not provided with such a function or its encryption protocol seems untrustworthy, the transmission between the centralized console and the agents should be protected from using outside programs.

Virtual Private Networks

What Is A VPN?

A VPN provides network connectivity over long physical distances. In this respect, a VPN is a specialized form of Wide Area Network (WAN). The key feature of a VPN, however, is its ability to use public networks like the Internet rather than rely on private leased lines. VPN technolo-

gies implement restricted-access networks that utilize the same cabling and routers as a public network, and they do so without sacrificing features or basic security.

A VPN supports at least three different modes of use:

- ▶ Remote access client connections
- ▶ LAN-to-LAN internetworking
- ▶ Controlled access within an intranet

VPN Technology

VPN technology is based on the idea of tunneling. Network tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.

For Internet-based VPNs, packets in one of several VPN protocols are encapsulated within IP packets. VPN protocols also support authentication and encryption to keep the tunnels secure.

Two Types of VPN Tunneling

VPN supports both voluntary and compulsory tunneling. Both types of tunneling can be found in practical use.

- ▶ In **VOLUNTARY TUNNELING**, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection.
- ▶ In **COMPULSORY TUNNELING**, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.

VPN Tunneling Protocols

Several interesting network protocols have been implemented specifically for use with VPN tunnels. The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

Point-to-Point Tunneling Protocol (PPTP)

Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in client support for this protocol. The

Module 2, Chapter 5

initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

Layer Two Tunneling Protocol (L2TP)

The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model -- thus the origin of its name.

Internet Protocol Security (IPSec)

IPSec is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution, or it can be used simply as the encryption scheme within L2TP or PPTP. IPSec exists at the network layer (Layer Three) in OSI.

The Future of VPN

The success of VPNs in the future depends mainly on industry dynamics. Most of the value in VPNs lies in the potential for businesses to save money. Should the cost of long-distance telephone calls and leased lines continue to drop, fewer companies may feel the need to switch to VPNs for remote access. Conversely, if VPN standards solidify and vendor products interoperate fully with other, the appeal of VPNs should increase.

The success of VPNs also depends on the ability of intranets and extranets to deliver on their promises. Companies have had difficulty measuring the cost savings of their private networks, but if it can be demonstrated that these provide significant value, the use of VPN technology internally may also increase.

Indian IT Act

In India, cyber laws are contained in the Information Technology, Act 2000. In May 2000, both the houses of Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President Of India in August 2000 (IT Act 2000).

The IT Act 2000 aims to provide the legal infrastructure for e-commerce in India. At this juncture, it is relevant to understand what the IT Act, 2000 offers and its various perspective.

This section attempts a brief review of provisions contained in the act and the possible implications.

- ▶ The main objective of the Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as

e-commerce, which involve the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies.

- ▶ Exemption/Exclusion. The Act shall not apply to the following categories of transaction:
 - ▼ (a) Any Negotiable Instrument; (b) A Power of Attorney; (c) the Trust; (d) A will including any other testamentary disposition; (e) Any contract for the sale or conveyance of immovable property; and (f) Any other documents or transactions as may be decided by the Central Government.

Digital Signatures [Chapter II]

With the passing of the Act, any subscriber (i.e., a person in whose name the Digital Signature Certificate is issued) may authenticate electronic record by affixing his Digital Signature. Electronic record means data record or data generated image or sound, stored, received or sent in an electronic form or microfilm or computer generated microfiche.

Electronic Governance [Chapter III]

Where any law provides submission of information in writing or in the type written or printed form, from now onwards it will be sufficient compliance of law, if the same is sent in an electronic form. Further, if any statute provides for affixation of signature in any document, the same can be done by means of digital signature.

Similarly, the filing of any form, application or any other document with the Government and issue or grant of any license, permit, sanction or approval and any receipt acknowledging payment can be done by the Government offices by means of electronic form. From now, onwards retention of documents, records, or information as provided in any law, can be done by maintaining electronic records. Any rule, regulation, order, by-law or notification can be published in the Official Gazette or Electronic Gazette.

The Act, however, provides that no Ministry or Department of Central Government or the State Government or any Authority established under any law can insist upon acceptance of document only in the form of electronic record.

Regulation of Certifying Authorities [Chapter IV]

The Central Government may appoint a Controller of Certifying Authority who shall exercise supervision over the activities of Certifying Authorities.

Certifying Authority means a person who has been granted a license to issue a Digital Signature Certificate. The Controller of Certifying Authority shall have powers to lay down rules, regulations, duties, re-

Module 2, Chapter 5

sponsibilities and functions of the Certifying Authority issuing Digital Signature Certificates. The Certifying Authority empowered to issue a Digital Signature Certificate shall have to procure a license from the Controller of Certifying Authority to issue Digital Signature Certificates. The Controller of Certifying Authority has prescribed detailed rules and regulations in the Act, as to the application for license, suspension of license and procedure for grant or rejection of license.

More on this can be found at the Controller of Certifying Authority's website: <http://www.cca.gov.in/>

Digital Signature Certificate [Chapter VII]

Any person may make an application to the Certifying Authority for issue of Digital Signature Certificate. The Certifying Authority while issuing such certificate shall certify that it has complied with the provisions of the Act.

The Certifying Authority has to ensure that the subscriber (i.e., a person in whose name the Digital Signature Certificate is issued) holds the private key corresponding to the public key listed in the Digital Signature Certificate and such public and private keys constitute a functioning key pair. The Certifying Authority has the power to suspend or revoke Digital Signature Certificate.

Penalties and Adjudication [Chapter IX]

If any person without the permission of the owner, accesses the owner's computer, computer system or computer network or downloads copies or any extract or introduces any computer virus or damages computer, computer system or computer network, data etc. he shall be liable to pay damage by way of compensation not exceeding Rupees One Crore to the person so affected.

Summary

This chapter deals with Network Security in detail and is a vital input for IS auditors.

A good understanding of the role of cryptography, security protocols, firewalls, Intrusion Detection Systems and Virtual Private Networks would help an auditor to check the adequacy of controls in a network and also help in recommending control features.

The chapter also updates the reader on the country's legal and regulatory framework.

Penetration testing is an important tool the auditors should learn about.

As with the previous chapters, here too we take the reader into realms of future: how is computer forensics shaping up?



Questions

1. An organization is about to implement a computer network in a new office building. The company has 200 users located in the same physical area. No external network connections will be required. Which of the following network configurations would be the MOST expensive to install?
 - A. Bus
 - B. Ring
 - C. Star
 - D. Mesh
2. In Wide Area Networks (WANs):
 - A. data flow must be half duplex
 - B. communication lines must be dedicated.
 - C. circuit structure can be operated only over a fixed distance.
 - D. the selection of communication lines will affect reliability.
3. An organization is considering installing a local area network (LAN) in a site under construction. If system availability is the main concern, which of the following topologies is MOST appropriate?
 - A. Ring
 - B. Line
 - C. Star
 - D. Bus
4. Which of the following is NOT an element of a LAN environment?
 - A. Packet switching technology
 - B. Baseband
 - C. Ring or short bus topology
 - D. Public circuit switching technology
5. Which of the following OSI layers communicates with the user programs?
 - A. Physical
 - B. Application
 - C. Presentation
 - D. Session
6. The advantage of a Ring topology is that
 - A. It is easy to install
 - B. It is easy to add or replace computers to the network
 - C. It minimizes network traffic congestion

Module 2, Questions

- D. It uses a number of high speed hubs and switches
- 7. An agreement between two computer systems related to methods of data transmission that is packed and interpreted is called
 - A. Communications channel
 - B. Communications protocol
 - C. Synchronous mode of transmission
 - D. Asynchronous mode of transmission
- 8. A session can be defined as
 - A. A link between two network nodes
 - B. Series of transmission without any disconnection
 - C. A specific place in a system
 - D. Bi-directional data flow between two network nodes.
- 9. Which of the following would typically be considered a LAN?
 - A. 10 computers in your office connected together and hooked up to a printer
 - B. A connection of one computer in Mumbai to another in Delhi
 - C. The city-wide connection between ATMs
 - D. The 3 stand-alone PCs in your home
- 10. Which network typically demands more knowledgeable users?
 - A. server-based network
 - B. peer-to-peer network
 - C. local area network
 - D. wide area network
- 11. All of the following are true relating to the use of fiber optics EXCEPT:
 - A. Data is transmitted rapidly
 - B. Fiber optic cable is small and flexible
 - C. They are unaffected by electrical interference
 - D. They provide the highest level of signal attenuation
- 12. A major problem in networking is the slow rate of data transfer. Which of the following would help counter this problem?
 - A. Data formatting
 - B. Allocating adequate bandwidth
 - C. Centralized control
 - D. All of the above
- 13. Which of the following can a local area network (LAN) administrator use to protect against exposure to illegal or unlicensed software usage by the network user?
 - A. Software metering
 - B. Virus detection software
 - C. Software encryption
 - D. Software decryption

Module 2, Questions

14. Which of the following devices connects two or more dissimilar computer systems by interpreting and translating the different protocols that are used?
 - A. Router
 - B. Repeater
 - C. Gateway
 - D. Firewall
15. The device primarily used to extend the network that must have the ability to act as a storage and forwarding device is a:
 - A. router
 - B. bridge
 - C. repeater
 - D. gateway
16. Which of the following transmission media would NOT be affected by cross talk or interference?
 - A. Fiber optic systems
 - B. Twisted pair circuits
 - C. Microwave radio systems
 - D. Satellite radio-link systems
17. Which of the following media would be MOST secure in a telecommunication network?
 - A. Dedicated lines
 - B. Base band network
 - C. Dial up
 - D. Broad band network digital transmission
18. Which of the following transmission media is MOST resistant to a sniffing attack?
 - A. Optical fiber
 - B. Satellite microwave
 - C. Twisted-pair wire
 - D. Infrared
19. A hub is a device that connects:
 - A. two LANs using different protocols.
 - B. a LAN with a WAN.
 - C. a LAN with a MAN.
 - D. two segments of a single LAN.
20. Which type of cable uses a BNC connector?
 - A. Twisted pair
 - B. UTP
 - C. STP
 - D. Coaxial cable

Module 2, Questions

21. An electronic device that combines data from several low speed communication lines into a single high speed line is called
 - A. Modem
 - B. Multiplexer
 - C. Channel
 - D. Link Editor
22. It is essential to monitor telecommunication processes and ensure that data transmission is complete and accurate. Which of the following automated processes / reports measure this?
 - A. Turnaround time reports
 - B. Help Desk response monitoring reports
 - C. Breakdowns/downtime reports
 - D. Online monitoring tools
23. Which of the following functions cannot be performed using a communications network control terminal?
 - A. Resetting queue lengths
 - B. Starting and terminating line processes
 - C. Generating a control total for a point of sale device
 - D. Correcting a hardware error in a modem
24. A service provided to businesses by telecommunication companies or long distance carriers that provides a permanent direct connection between two geographically separate local area networks is called a:
 - A. Point-to-point link
 - B. Message switching
 - C. Distributed network
 - D. Packet switching
25. A transmission technique in which a complete message is sent to a concentration point for storage and routing to the destination point when a communication path is available is called:
 - A. Circuit Switching
 - B. Message Switching
 - C. Packet Switching
 - D. Junction Switching
26. All of the following are considered characteristics of N-Tier computing architecture EXCEPT:
 - A. Distributed computing
 - B. Open Industry standards
 - C. Thin Client interfaces
 - D. Monolithic architecture

Module 2, Questions

27. Measuring utilization of all important network resources so that individual or group uses on the network can be regulated appropriately is called:
- A. Performance management
 - B. Security management
 - C. Accounting management
 - D. Configuration management
28. Which of the following is most often used for collecting statistical and configuration information about network devices such as computers, hubs, switches, routers, etc.?
- A. Simple Network Management Protocol
 - B. Online reports
 - C. Downtime reports
 - D. Help desk reports
29. Which of the following would typically be considered the fastest to restore?
- A. Normal backup
 - B. Incremental backup
 - C. Differential backup
 - D. Copy backup
30. All the following are phases in the establishment of a Switched Virtual Circuit EXCEPT:
- A. Circuit termination
 - B. Data transfer
 - C. Circuit expansion
 - D. Circuit establishment
31. Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?
- A. Gateway
 - B. Protocol converter
 - C. Front-end communication processor
 - D. Concentrator/multiplexer
32. An IS auditor performing a telecommunication access control review would focus his / her attention MOST on the:
- A. maintenance of usage logs of various system resources
 - B. authorization and authentication of the user prior to granting access to system resources
 - C. adequate protection of stored data on servers by encryption or other means.
 - D. accountability system and the ability to properly identify any terminal accessing system resources.

Module 2, Questions

33. Which of the following controls would be MOST comprehensive in a remote access network with multiple and diverse sub-systems?
- A. Proxy server
 - B. Firewall installation
 - C. Network administrator
 - D. Password implementation and administration
34. A reasonably controlled practice in the distributed executable programs that execute in background of a web browser client, like Java applets and ActiveX controls, is:
- A. installation of a firewall
 - B. usage of a secure web connection
 - C. acceptance of executable only from the established and trusted source
 - D. hosting the website as part of your organization
35. When an organization's network is connected with an external network in an Internet client-server model not under that organization's control, security becomes a concern. In providing adequate security in this environment, which of the following assurance levels is LEAST important?
- A. Server and client authentication
 - B. Data integrity
 - C. Data recovery
 - D. Data confidentiality
36. In a TCP/IP based network, an IP address specifies a:
- A. Network connection.
 - B. Router/gateway.
 - C. Computer in the network.
 - D. Device on the network such as a gateway/router, host, server, etc.
37. In Internet architecture, a domain name service (DNS) is MOST important because it provides the:
- A. Address of the domain server.
 - B. Address of the naming client.
 - C. Resolution of the name to the IP address on the Internet.
 - D. Domain name characteristics.
38. In an Internet URL, "http://www.infosys.com", what does the ".com" signify?
- A. Identifies the protocol being used
 - B. Identifies that the site is on the Internet
 - C. It is an additional information and is not needed
 - D. Identifies the purpose of the site. It stands for commercial.

Module 2, Questions

39. In which of the following, tags are placed within text to accomplish document formatting, visual features such as font size, italics and bold, and the creation of links:
- A. FTP
 - B. HTTP
 - C. Telnet
 - D. ActiveX
40. Which of the following allow users on the Internet to communicate with each other by typing text mode in real time:
- A. IM
 - B. RFC
 - C. FYI
 - D. FAQ
41. A firewall access control list may filter access based on each of the following parameters EXCEPT:
- A. port.
 - B. service type.
 - C. network interface card (NIC)
 - D. internet protocol (IP) address.
42. Which of the following is not provided by a public key infrastructure (PKI)?
- A. Access control
 - B. Network Reliability
 - C. Authentication
 - D. Non-Repudiation
43. Secure socket layer (SSL) protocol addresses the confidentiality of a message through:
- A. symmetric encryption
 - B. message authentication code
 - C. hash function
 - D. digital signature certificates
44. Electromagnetic emissions from a terminal represent an exposure because they:
- A. affect noise pollution.
 - B. disrupt processor functions.
 - C. produce dangerous levels of electric current.
 - D. can be detected and displayed
45. Which of the following would an IS auditor consider a MAJOR risk of using single sign-on in a networked environment?
- A. It enables access to multiple applications
 - B. It represents a single point of failure
 - C. It causes an administrative bottleneck

Module 2, Questions

- D. It leads to a lockout of valid users
46. All of the following are significant Internet exposures EXCEPT:
- A. Loss of integrity
 - B. Denial of Service attacks.
 - C. Insufficient resources to improve and maintain integrity
 - D. Unauthorized access
47. A manufacturer has been purchasing materials and supplies for its business through an e-commerce application. Which of the following should this manufacturer rely on to prove that the transactions were actually made?
- A. Reputation
 - B. Authentication
 - C. Encryption
 - D. Non-Repudiation
48. An IS auditor who intends to use penetration testing during an audit of Internet connections would:
- A. evaluate configurations.
 - B. examine security settings.
 - C. ensure virus-scanning software is in use.
 - D. use tools and techniques that are available to a hacker
49. A sequence of bits appended to a digital document that is used to authenticate an e-mail sent through the Internet is called a:
- A. digest signature
 - B. encrypted message
 - C. digital signature
 - D. hash signature
50. Which of the following provides the GREATEST assurance in achieving message integrity and non-repudiation ?
- A. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the message digest.
 - B. The recipient uses his private key to decrypt the secret key
 - C. The encrypted message digest and the message are encrypted using a secret key
 - D. The encrypted message digest is derived mathematically from the message to be sent

Answers

QUESTION No	1	2	3	4	5	6	7	8	9	10
ANSWERS	D	D	C	D	B	C	B	B	A	B

Module 2, Questions

QUESTION No	11	12	13	14	15	16	17	18	19	20
ANSWERS	D	D	B	A	C	A	A	A	D	D

QUESTION No	21	22	23	24	25	26	27	28	29	30
ANSWERS	B	D	D	A	B	D	C	A	A	C

QUESTION No	31	32	33	34	35	36	37	38	39	40
ANSWERS	A	B	D	C	C	A	C	D	B	A

QUESTION No	41	42	43	44	45	46	47	48	49	50
ANSWERS	C	B	A	D	B	C	D	D	C	A



Module 3: Protection of Information Assets

1 Introduction to Information Assets

✂ Learning Goals ✂

To understand:

- ▶ The difference between Information Asset and Information Systems Asset
- ▶ Classification of Resources
- ▶ Classification of Users
- ▶ Access Control Models
- ▶ Computer Crime

Introduction

The first major process undertaken in protecting information assets is Information Classification. All information in the company should be classified according to its intended audience, and handled accordingly. This includes paper documents, computer data, faxes and letters, audio recordings, and any other type of information. Classifying this information and labelling it clearly helps employees understand how management expects them to handle the information, and to whom they should expose the information.

After classifying information, the next process is the classification of users. The classification of users is based on the roles played by the users in the organisation. And lastly, access control models describe the what kind of users can have access to what kind of data.

Information Classification

The Information Classification process focuses on business risk and data valuation. Not all data has the same value to an organization. Some data is more valuable to the people who are making strategic decisions because it aids them in making long-range or short-range business direction decisions. Some data, such as trade secrets, formulas, and new product information, are so valuable that its loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility.

For these reasons, information classification has an enterprise-level benefit. Some of the other benefits are as follows:

Module 3, Chapter 1

- ▶ Demonstrates an organization's commitment to security protections
- ▶ Helps identify which information is the most sensitive or vital to an organization
- ▶ Supports the tenets of confidentiality, integrity, and availability as it pertains to data
- ▶ Helps identify which protections apply to which information
- ▶ Might be required for regulatory, compliance, or legal reasons

Information Asset Vs. Information Systems Asset

An "Information Asset" is a any definable piece of information, which the organisation regards as "valuable". Information Assets usually have one or more of the following characteristics:

- ▶ They are recognised to be of value to the organisation.
- ▶ They are not easily replaceable without cost, skill, time, resources or a combination of these resources.
- ▶ They form a part of the organisation's corporate identity, without which, the organisation may be vulnerable to a variety of threats.

The purpose of Information Security to identify the threats against, the risks and the associated potential damage to, and the safeguarding of Information Assets. The information which comprises an Information Asset, may be nothing more than name a of potential customer; or it may be research data; or even a new packaging design.

An "information systems asset" is the computer systems and information sources used by an organisation to support its day to day operations.

Integrity, Availability and Confidentiality

In the information security field, integrity is often defined more narrowly as having two facets: data (the information asset) integrity and system (Information System Asset) integrity.

DATA INTEGRITY is the requirement that information and programs are changed only in a specified and authorized manner.

SYSTEM INTEGRITY is the requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

AVAILABILITY is the requirement intended to assure that systems work promptly and service is not denied to authorized users.

CONFIDENTIALITY is the requirement that private or confidential information not be disclosed to unauthorized individuals.

System Effectiveness and System Efficiency

System effectiveness is defined as the extent to which information technology processes produce desired objectives. One purpose of controls is to support and improve processes, through detecting and correcting process failures. There is often a positive correlation between strong controls and effective processes. Effectiveness is measured on the basis of key performance indicators for process. For example, a measure of the effectiveness of software release management is the percent of releases built and implemented on schedule. Another example is the percent of production servers that match their intended state. A combined effectiveness score can be created based on a range of effectiveness measures to measure overall process effectiveness.

Efficiency is defined as the extent of information-technology resources used and needed to achieve the desired objective. In addition to improving process effectiveness, strong controls will positively affect process efficiency. By preventing deviations from approved processes, the cost of these processes is likely to be reduced. System efficiency is based on the costs and time of providing processes. These costs include direct costs, such as staff wages, and indirect costs (such as lost productivity) if a process fails.

For both system effectiveness and system efficiency, maintenance of system integrity is a prerequisite. While access controls are predominantly designed to ensure system integrity, they also indirectly help in achieving system effectiveness and system efficiency. In order to achieve basic business objectives, system integrity, system effectiveness and system efficiency are required.

Classification of Information Assets

Access Controls enable authorised users or processes (commonly referred to as the subjects) gain access to Information and Information Systems ("IS") assets or resources (commonly referred to as objects). Different kinds of IS assets may require different degree of access controls. Further, within an asset (say, a database), different elements or components of the asset (individual fields or records meeting a certain criteria) may require more stringent controls. For example a bank manager may have rights to modify the borrower's database with regard to credit limit of a borrower but not have access to modify cash transactions in the cash database. Hence information and computer processes, in an organisation, may have different degrees of criticality. Information systems resources may require to be classified or categorized according to their sensitivity. This would depend upon the risks affecting such resources and impact resulting from exposure. Such classification makes for administrative convenience of implementing and maintaining access control systems and importantly optimising the cost of security.

Module 3, Chapter 1

Some information is more critical to a business than others such as production process information, formulas, strategic plans, research information. In the financial services industry, for example, information assets are very close to being financial assets. The loss of such information can jeopardize the existence of the business or create loss of goodwill and trust among stakeholders and loss of brand equity. Compared to this, the organisation may also have information, which are of less consequence in the event of their loss, such as a list of customers, details of employee pay, etc. Thus in order to ensure cost-effective controls, it is beneficial to classify the entire organisational information. This also enables fine tuning of access control mechanisms and avoids the cost of over-protecting and under-protecting information.

IS resource classification also helps in determining the degree of access to be authorised to a user with regard to various classes of resources rather than the tedious task of assessing the extent of access in respect of every IS resource. For example, access to production or live programs and data should be restricted to a limited set of users. Similarly, access to test data and programs in the development area, must be restricted to identified group of programmers and analysts.

The scheme of classification may vary depending on the type of organisation. However some standard or popular classifications are also available. Data in high security organisations such as defence establishments may be classified on the following lines:

- ▶ **TOP SECRET:** This indicates the highest classification wherein the compromise of the confidentiality, integrity and availability can endanger the existence of the organisation. Access to such information may be restricted to either a few named individuals in the organisation or to a set of identified individuals.
- ▶ **SECRET:** Information in this category is strategic to the survival of the organisation. Unauthorized disclosure could cause severe damage to the organisation and stakeholders.
- ▶ **CONFIDENTIAL:** Information in this category also needs high levels of protection but unauthorized disclosure may cause significant loss or damage. Such information is highly sensitive and should be well protected.
- ▶ **SENSITIVE:** Such information requires higher classification as compared to unclassified information. Disclosure may cause serious impact.
- ▶ **UNCLASSIFIED:** Information that does not fall in any of the above categories finds place here. This also implies that the nature of the information is such that its unauthorized disclosure would not cause any adverse impact on the organisation. Such information may also be made freely available to the public.

Another type of classification, popular in commercial organisations, can be: Public, Sensitive, Private and Confidential.

Data Privacy and Data Protection

Many advanced nations have enacted legislations concerning “Data Privacy”. These often take the form of prohibiting release of medical or other information to third parties without a court order. Regulatory bodies also require restriction on dissemination of data collected by certain industries, notably banks and financial services.

The UK’s Data Protection Act, 1988, for example has the following key features:

- ▶ The legislation is not limited specifically to data held electronically: it now applies to all personal information held in “relevant filing systems”, which may be in **ANY** medium (paper, database, spreadsheet, word-processing folder, etc.). The criteria for whether something is a “filing system” in the terms of the Act relate to whether the information is held in a structured way, indexed by individual identifiers. In essence, any file held specifically on a particular individual should now be regarded as subject to the legislation.
- ▶ There is an emphasis on giving data subjects advance notification about the data being collected and what will be done with it (how it is to be ‘processed’). In this context, data subjects must have the opportunity to consent to the collection and processing of their data. That consent should be informed, given freely, and (wherever possible) be obtained explicitly and in advance.
- ▶ There are “Fair Processing” principles. The personal data that is collected and processed must be for specified, explicit and legal purposes, and the data held must be accurate, relevant and not excessive to those purposes. Personal data must be kept secure, up-to-date and not longer than actually necessary.
- ▶ There are strict controls on the processing of ‘sensitive personal data’ (i.e. race, ethnicity, gender, health), even where it is processed only for research purposes.

The Act also prescribes compliance audits. The aims of data protection compliance audits go beyond the basic requirements of say Data Security and address wider aspects of data protection including:

- ▶ Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
- ▶ Quality Assurance – ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
- ▶ Retention – appropriate weeding and deletion of information.
- ▶ Documentation on authorised use of systems, e.g. codes of practice, guidelines etc.
- ▶ Compliance with individual’s rights, such as subject access.

- ▶ Compliance with the data protection legislation in the context of other pieces of legislation.

Classification of Users

Entitlement of access to an information resource and degree of access is determined based on the job description, functions and role of the user in the organisation. The rights of access authorised to the user should be such as to ensure that the user does not gain access to undesired information resources or undesired mode of access to the information resource. This is governed by the “need to know and need to do basis” or the principle of least privileges. The principle of least privilege (also known as the principle of least authority) is an important concept in information security. It advocates for minimal user profile privileges on computers, based on users’ job necessities. It can also be applied to processes on the computer; each system component or process should have the least authority necessary to perform its duties. This also called the “default deny” principle. All these terms imply that access is available only to users after it has been specifically granted to them, presumably by the data owner (defined below) and that no more access than is necessary to perform the job function has been granted to them.

These principles helps reduce the “attack surface” of the computer by eliminating unnecessary privileges that can result in network exploits and computer compromises. At the same time, the authority for access should be adequate so as not the adversely effect the functioning of the user.

Based on the these principles users can be broadly classified as:

Data Owners: In an organisation, ownership is established for every data resource. This enables assignment of accountability and responsibility for every data resource. The owner is responsible for protection of the data resource and accountable for any loss or damage to the data resource. For example, the Sales Director may be the designated owner of the sales transaction database. The data owner has the rights of determining the classification of the data resource or changes thereto and rights of delegation of responsibilities to users and custodians. However, custodians may be responsible for day to day protection of the data resource, under delegated authority from owners.

Data Users: Users require access to the data for their day to day functioning, e.g. employees other than designated data owners, data entry operators, customers etc. Data users derive their rights of access from the data owners. Users are governed by the security policy and procedures of the organisation and have the responsibility to use their authority for organisational purposes and protect the resources.

Data Custodians: The custodians e.g. the IT Department are delegated with the responsibility of administration including protection of data resources. The custodians also derive their rights from the owners and their actions are governed by the security policy framework, policies and procedures.

Naming Conventions

The classifications once done, govern the security administration in determining which class of information can be accessed by which class of users and to what degree or type of access. For example in a bank, the access to information about internal credit rating of borrowers contained in some of the central servers will be restricted to managers of particular department, possibly spread geographically across the country. However, only a designated subset of these managers may have access to modify the information. For purposes of ease of administration and efficient access control, such category of information would need to be identified by a specified name, e.g. "Class A" and the category of users can be classified as "Group One". The access control policy could clearly define the access rights to each of the category of resources with regard to the user groups.

Based on the granularity of access control desired, the naming conventions can be applied. These conventions simplify the access rules make it easy to maintain.

The roles of various office-bearers, like Database Administrator, Systems Administrator are covered in Module 6.

Access Control Models

One of the critical challenges in implementing access control systems is to configure the appropriate access rules when a subject seeks to access an object or objects. This is often problematic since the access control should protect the IS resources and at the same time ensure that eligible persons and processes have rightful access to resources.

Management evolves policy for systems, sub-systems, applications or group of systems. Logical access controls are a technical means of implementing policy decisions. The development of an access control policy is often challenging since it requires balancing of interests of security, operational requirements, and user-friendliness.

While there are many access control models, the two basic ones are discussed below:

Mandatory Access Control: Also referred to as labelled security, access restrictions are associated with every resource and every user. An individual user is given access to a resource only based on his clearance for that particular degree or level of security with respect to every resource.

Module 3, Chapter 1

Such kind of security is usually applicable in the case of defence installations, wherein a user cleared for a higher level of security does not necessarily by default get rights of access to the lower levels of security but instead his need to know determines his right of access. Hence such access is rule-based, dependent on the access rights of the user and the access rights for a resource and the identity of an individual is immaterial. Mandatory access control requires that each IS resource be classified and every user be assigned a clearance level. E.g. A user will not have access to a database unless his user-id possesses the clearance level greater or equal to the database's classification.

Discretionary Access Control: This represents the other extreme to mandatory access, wherein users are given rights to specify delegation of rights to resources allowed to them. After the initial allocation of rights of access to resources to an individual, the individual possess the rights to specify the delegation of access rights to other users and specify the degree of access as well. Such a model is more popular in commercial organisations. For example, a Project Manager assigned with a software project in a software company is allotted a set of rights to access to certain resources, based on which she has the discretion to delegate access within her allocated resources to other users. However, such delegation may be restricted based on content or context and monitored by security administrator.

Computer Crime

Where an organisation has failed to take information security seriously it may end up becoming an unwitting accomplice to computer crime.

While on one hand, computers have been a significant contributor in enhancing the quality of business operations and human lives, on the other hand they have also facilitated easier and faster means of perpetrating crimes. The Organisation of Economic Co-operation and Development defines Computer Crime as “any illegal, unethical or unauthorized behaviour relating to the automatic processing and transmission of data”. This covers both the information asset and the information systems asset.

Computer crimes offer a great attraction to perpetrators of crime due to certain advantages:

- ▶ Extreme difficulty in tracing the perpetrator's identity
- ▶ Most Cyber crimes require only logical access to the target computer system
- ▶ Negligible cost of perpetration
- ▶ Newer and easier methods of perpetrating crime
- ▶ Crimes can be committed at unbelievable speed and cover the globe
- ▶ Criminals get together to form virtual organisations for exchange of information on crime targets.

- ▶ Lack of a accepted global legal structure for prevention of computer crimes and prosecution of criminals.

The impact of computer crime can be any of the following:

- ▶ **Financial Loss:** Even though slow, the growth of monetary transaction processing systems fuelled by electronic commerce has resulted in much of the financial operations such as shopping, banking, employee payments, vendor payments being significantly automated and networked. Direct monetary losses to businesses result due to financial frauds such as stealing of bank balances and credit card numbers. Besides with every successful attack, significant sums are required to be spent to recover from damage, refurbish the dented image due to computer crime and legal penalties.
- ▶ **Legal Implications:** An organisation is governed by numerous laws and regulations. Electronic commerce including automation of business processes presents newer risks, which directly or indirectly impact the organisation. While the perpetrator of crime is protected, organisations suffer from legal action from customers, vendors, employees and other stakeholders due to consequences of computer crime and resultant losses and damage therefrom. Medical and financial organisations are required by law or regulations to preserve the confidentiality of their constituents information. Inability to do so might invite civil or disciplinary action by the concerned regulatory body. Access controls seek to mitigate these risks.
- ▶ **Loss of Credibility or Competitive Edge:** An organisation's success depends, to a significant extent, on maintaining its competitive edge through quality of its service, customer relations, global reach, innovative practices. Banks and financial service companies require intensive care in ensuring customer confidence. One single computer crime incident could shatter the business image and customer confidence resulting in long term adverse effects for the business. These risks increase significantly while business is conducted online via the Internet or via extranets.
- ▶ **Cyber Espionage and blackmail:** Undesired disclosure of sensitive information can result in the perpetrator blackmailing the organisation. Competitors can access sensitive business information resulting in compromising the growth and prospects of the organisation.
- ▶ **Sabotage:** Perpetrators may not be interested in personal financial gain but are interested in spoiling the credibility and prospects of the organisation or simply disrupting the business.
- ▶ **Privacy and Confidentiality:** Computers hold several types of information about a range of stakeholders and sensitive information relating to the organisation. The undesired disclosure or access of such information to the public can lead to severe embarrassment and legal repercussions, besides loss of image.

Module 3, Chapter 1

In the Indian context, Section 43 of The Information Technology Act, 2000 prescribes the penalty for damage to computer, computer system, etc. It reads as follows:

“If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, —

- ▶ accesses or secures access to such computer, computer system or computer network;
- ▶ downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- ▶ introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- ▶ damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
- ▶ disrupts or causes disruption of any computer, computer system or computer network;
- ▶ denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
- ▶ provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
- ▶ charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

he shall be liable to pay damages by way of compensation not exceeding One Crore rupees to the person so affected.”

The following explanations are appended to Section 43.

- ▶ "computer contaminant" means any set of computer instructions that are designed—
 - ▼ to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
 - ▼ by any means to usurp the normal operation of the computer, computer system, or computer network;
- ▶ "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

- ▶ "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- ▶ "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

While the Information Technology Act is punitive in nature, access controls are intended to be preventive in nature. Commission of a computer crime implies circumvention of access controls. Since there is no such thing as foolproof security, access controls are intended to make computer crime unprofitable or uneconomic by making the cost or effort of circumventing the control greater than the potential reward.

Computer Forensics

Computer Crime is hard to detect and much harder to prove. The most severe computer crimes are committed and facilitated by gaining logical access to computer systems and networks. Unlike non-computer crimes, the perpetrator does not leave any physical marks or trails, evidence, if any, is usually in electronic form. Besides evidence in electronic form is capable of undetectable tampering, which makes it untenable in the court of law.

Computer forensics is a specialized field which deals with the employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity. This is critical to secure legal evidence to bring the perpetrators to the book. This requires preservation, identification, extraction and documentation of computer evidence.

The computer forensics process consists of three phases: acquisition, examination, and utilization. Computer forensic investigators must have software tools that can effectively and efficiently accomplish the following tasks:

- ▶ Image data
- ▶ Create comprehensive file listings
- ▶ Identify and recover text located anywhere on the storage media
- ▶ View text and image files
- ▶ Assure that recovery methods do not unnecessarily contaminate data evidence
- ▶ Identify compressed data and decompress it
- ▶ Identify encrypted files

Perpetrators of computer crimes

The common perpetrators of computer crimes are:

- ▶ Hackers: Persons with computing talent who gain unauthorized access to computers and networks. Hackers explore systems to locate loopholes and security vulnerabilities to gain access. However hackers are not always criminally motivated, many hack into systems just for the challenge of breaking in or for fun. Social or anti-social activists may use hacking to gain unauthorized access to systems to spread their message. Hackers with criminal intent either hacking for money or to cause damage are called crackers.
- ▶ Employees:
 - ▼ IS Personnel: IS personnel often have greater and more privileged access to IS resources, capable of misuse.
 - ▼ Disgruntled employees looking to vent their ire often find it easier to gain logical access to cause damage or sabotage operations.
 - ▼ Employees who are addicted to substances or with financial problems could scavenge for sensitive organisational information to be sold to outsiders or gain access to privileged information for disclosure to competitors.
- ▶ Accidental Ignorant: Users may gain accidental(i.e. non-malicious) access to sensitive areas or sensitive computer functions.
- ▶ Others include end users, part time and temporary personnel, former employees, outsiders like competitors, foreigners, organised criminals, terrorists, vendors and consultants

Summary

The information asset is the organisational data and the mediums and devices of storage, processing and communications constitute the Information system asset. Inadequate protection to either information asset or the information system assets may result in computer crime.

Information systems resources are required to be classified or categorized according to their sensitivity. This depends upon the risks affecting such resources and impact resulting from exposure. The classifications once done, governs the security administration in determining which class of information can be accessed by which class of users and to what degree of access further governed by the set of access rules. The scheme of classification may vary depending on the type of organisation. In commercial organisations, data may be classified as public, sensitive, private or confidential. Once users and resources are classified, it then becomes possible to specify which users can access what data. The two broad frameworks available are the mandatory access control and discretionary access control.

Module 3, Chapter 1

Any unauthorized behaviour relating to the automatic processing and transmission of data is called computer crime.



2 Information Security Policy

✂ Learning Goals ✂

To understand:

- ▶ Security Policy
- ▶ Tools to Implement Policy
- ▶ Components of Policies
- ▶ Policy Implementation

Introduction

A security policy is the statement of intent by the management about how to protect a company's information assets information system assets. In its basic form, a security policy is a document that describes a company's or organization's security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that will help protect a company's assets and its ability to conduct business.

A security policy is the essential foundation for an effective and comprehensive security program. A security policy is the primary way in which management's expectations for security are translated into specific measurable and testable goals and objectives. It provides guidance to the people who are building, installing, and maintaining computer systems, so they don't have to make those decisions by themselves. Security policies often include rules intended to:

- ▶ Preserve and protect information from any unauthorized modification, access or disclosure.
- ▶ Limit or eliminate potential legal liability from employees or third parties.
- ▶ Prevent waste or inappropriate use of organization resources

A security policy should be in written form. It provides instructions to employees about what kinds of behaviour or resource usage are required and acceptable, and about what is forbidden and unacceptable. A security policy gives clear instructions to IT staff and security professionals about how to restrict authority and enact access controls, authentication methods, privacy practices, and accounting techniques. A security policy also provides information for all employees about how to help protect their employer's assets and information, and it provides instructions regarding acceptable (and unacceptable) practices and behaviour.

Definition

The term information security policy is defined broadly as the documentation of computer security decisions. In making these decisions, managers face hard choices involving resource allocation, competing objectives, and organizational strategy related to protecting both technical and information resources as well as guiding employee behaviour. Managers at all levels make choices that can result in policy, with the scope of the policy's applicability varying according to the scope of the manager's authority. In this chapter we use the term policy in a broad manner to encompass all of the types of policy described above regardless of the level of manager who sets the particular policy. Managerial decisions on computer security issues vary greatly. To differentiate among various kinds of policy, this chapter categorizes them into three basic types:

- ▶ **PROGRAM POLICY** is used to create an organization's computer security program.
- ▶ **ISSUE-SPECIFIC POLICIES** address specific issues of concern to the organization.
- ▶ **SYSTEM-SPECIFIC POLICIES** focus on decisions taken by management to protect a particular system.

Familiarity with various types and components of policy will aid managers in addressing computer security issues important to the organization. Effective policies ultimately result in the development and implementation of a better computer security program and better protection of systems and information.

It is not important that one categorizes specific organizational policies into these three categories; it is more important to focus on the functions of each.

Procedures, standards, and guidelines are used to describe how these policies will be implemented within an organization. Further, while policies are approved at the topmost level, procedures, standards and guidelines are approved at lower levels of management. What is included in a policy may vary from organisation to organisation. Also note that, an item covered in a policy in one organisation may be documented at the procedure or standard level in another organisation.

Tools to Implement Policy: Standards, Guidelines, and Procedures

Because policy is written at a broad level, organizations also develop standards, guidelines, and procedures that offer users, managers, and others a clearer approach to implementing policy and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems. Procedures are yet more detailed

steps to be followed to accomplish particular security related tasks. Standards, guidelines, and procedures may be promulgated throughout an organization via handbooks, regulations, or manuals.

Organizational standards (not to be confused with national or international standards) specify uniform use of specific technologies, parameters, or procedures when such uniform use will benefit an organization. Standardization of organization-wide identification badges is a typical example, providing ease of employee mobility and automation of entry/exit systems. Standards are normally compulsory within an organization. Guidelines assist users, systems personnel, and others in effectively securing their systems. The nature of guidelines, however, immediately recognizes that systems vary considerably, and imposition of standards is not always achievable, appropriate, or cost-effective. For example, an organizational guideline may be used to help develop system-specific standard procedures. Guidelines are often used to help ensure that specific security measures are not overlooked, although they can be implemented, and correctly so, in more than one way.

Procedures normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task (e.g., preparing new user accounts and assigning the appropriate privileges). Some organizations issue overall computer security manuals, regulations, handbooks, or similar documents. These may mix policy, guidelines, standards, and procedures, since they are closely linked. While manuals and regulations can serve as important tools, it is often useful if they clearly distinguish between policy and its implementation. This can help in promoting flexibility and cost-effectiveness by offering alternative implementation approaches to achieving policy goals.

Program Policy

The senior management, issues program policy to establish (or restructure) the organization's computer security program and its basic structure. This high-level policy defines the purpose of the program and its scope within the organization; assigns responsibilities (to the computer security organization) for direct program implementation, as well as other responsibilities to related offices; and addresses compliance issues.

Program policy sets organizational strategic directions for security and assigns resources for its implementation.

Components of Program Policy

The following is a list of components found in a typical Information security program policy.

Module 3, Chapter 2

Purpose. Program policy normally includes a statement describing why the program is being established. This may include defining the goals of the program. Security-related needs, such as integrity, availability, and confidentiality, can form the basis of organizational goals established in policy. A primary purpose of program-level policy is to establish the IT security program. This includes defining the program management structure, the reporting responsibilities, the roles of individuals and groups throughout the organization, and the organization-wide goals of the security program. For instance, in an organization responsible for maintaining large mission-critical databases, reduction in errors, data loss, data corruption, and recovery might be specifically stressed. In an organization responsible for maintaining confidential personal data, however, goals might emphasize stronger protection against unauthorized disclosure.

Additionally, program-level policy should serve the purpose of emphasizing to all employees the importance of IT security and clarifying the individual employee's role and responsibilities. IT security policy may be met with a degree of scepticism unless given appropriate visibility and support by top management, and that visibility and support should be clearly and energetically reflected in the program-level policy and in its emphasis on employee participation.

The program-level policy should thus firmly establish individual employee accountability. Employees should be made aware via the policy that even if they are not designated IT security program personnel, they nonetheless have significant IT security responsibilities.

Scope. Program-level policy should be of sufficient breadth of scope to include all of the organization's IT resources, including facilities, hardware, software, information, and personnel. In some instances, it may be appropriate for a policy to name specific assets, such as major sites, installations, and large systems. In addition to such specified assets, it is important to include an overview of all of the types of IT resources for which the organization is responsible, such as workstations, Local Area Networks (LANs), standalone microcomputers, etc. In some instances, it may be appropriate for an organization's computer security program to be more limited in scope.

Responsibilities. Once the security program is established, its management is normally assigned to either a newly created or existing office. The responsibilities of officials and offices throughout the organization also need to be addressed, including line managers, applications owners, users, data processing centre manager, and the computer systems security group.

This section of the policy statement, for example, would distinguish between the responsibilities of computer services providers and those of the managers of applications using the provided services. The policy could also establish operational security offices for major systems, particularly those at high risk or most critical to organizational operations. It also can serve as the basis for establishing employee accountability. In assigning responsibilities, it is necessary to be specific; such statements as “computer security is everyone’s responsibility,” in reality, mean no one has specific responsibility.

At the program level, responsibilities should be specifically assigned to those organizational elements and officials responsible for the implementation and continuity of the computer security policy. Overall, the program-level assignment of responsibilities should cover those activities and personnel who will be integral to the implementation and continuity of the IT security policy.

The following are some of the personnel that are involved.

- ▶ **IT Security Program Manager:** IT security program managers are responsible for developing enterprise standards for IT security (e.g. single sign-on, remote access, user-id creation). They play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize IT security risks to the organization. They coordinate and perform system risk analyses, analyse risk mitigation alternatives, and build the business case for the acquisition of appropriate security solutions (including IT security services) that help enable mission accomplishment in the face of real world threats. These IT security program managers also support senior management in ensuring that security management activities are conducted as required to meet the needs of the organization.
- ▶ **Chief Information Officer:** The CIO is responsible for the organization’s IT planning, budgeting, investment, performance and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in procuring the most efficient and effective security product to fit the IT security architecture.
- ▶ **IT Investment Board:** The IT investment board (or its equivalent) is responsible for managing the capital planning and investment control process. This board can set the investment criteria for security product selection from qualitative and quantitative perspectives. The board can review benefits and risks for procuring a particular product and can be involved in examining alternative approaches.
- ▶ **IT System Security Officer:** The IT System Security Officer is responsible for ensuring the security of an information system throughout its life cycle. He is required to:

Module 3, Chapter 2

- ▼ Develop security policies and keep these policies up-to-date considering the changed business requirements, technology and threats.
- ▼ Help business in developing guidelines and procedures for implementation of security policy.
- ▼ Ensure that the risk acceptance process is followed when an exception to a security policy is necessitated.
- ▼ Remain current and up-to-date in technology and threats and security. So that he can meet the everyday security challenges and plan the security solutions in a better way.
- ▼ Understand the business processes so that appropriate security mechanisms can be applied.
- ▼ Work closely with systems administrators, security auditors, legal experts, insurance experts, etc to implement the security programmes effectively.
- ▼ Co-ordinate or assist in the investigation of security threats.
- ▼ Define the key threats to each asset.
- ▼ Help the management in the formulation of response to the security audit
- ▼ Help in disaster recovery.

Compliance. Without a formal, documented information security policy, it is not possible for management to proceed with the development of enforcement standards and mechanisms. Program-level policy serves as the basis for enforcement by describing penalties and disciplinary actions that can result from failure to comply with the organization's IT security requirements. Discipline commensurate with levels and types of security infractions should be discussed.

Program policy typically will address two compliance issues:

- ▶ General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components. Often an oversight office is assigned responsibility for monitoring compliance, including how well the organization is implementing management's priorities for the program.
- ▶ The use of specified penalties and disciplinary actions. Since the security policy is a high-level document, specific penalties for various infractions are normally not detailed here; instead, the policy may authorize the creation of compliance structures that include violations and specific disciplinary action(s).

Consideration should also be given to the fact that non-conformance to policy can be unintentional on the part of employees. For example, non-conformance can often be due to a lack of knowledge or training. It can also be the result of inadequate communication and explanation of the policy. For these reasons, it is desirable that, along with enforce-

ment, program-level policy make provisions for orientation, training, and compliance within a realistic timeframe.

Issue-Specific Policy

Whereas program policy is intended to address the broad organization-wide computer security program, issue-specific policies are developed to focus on areas of current relevance and concern to an organization. Management may find it appropriate, for example, to issue a policy on how the organization will approach contingency planning (centralized vs. decentralized) or the use of a particular methodology for managing risk to systems. A policy could also be issued, for example, on the appropriate use of a leading-edge technology, whose security vulnerabilities are still largely unknown, within the organization. Issue-specific policies may also be appropriate when new issues arise, such as when implementing a recently passed law requiring additional protection of particular information. Program policy is usually broad enough that it does not require much modification over time, whereas issue-specific policies are likely to require more frequent revision as changes in technology and related factors take place.

Components of Issue-Specific Policy

A useful structure for issue-specific policy is to break the policy into its basic components.

Issue Statement. To formulate a policy on an issue, managers first must define the issue with any relevant terms, distinctions, and conditions included. It is also often useful to specify the goal or justification for the policy which can be helpful in gaining compliance with the policy.

Statement of the Organization's Position. Once the issue is stated and related terms and conditions are defined, this section is used to clearly state the organization's position (defined management's decision) on the issue. To continue the previous example, this would mean stating whether use of unofficial software as defined is prohibited in all or some cases, whether there are further guidelines for approval and use, or whether case-by-case exceptions will be granted, by whom, and on what basis.

Applicability. Issue-specific policies also need to include statements of applicability. This means clarifying where, how, when, to whom, and to what a particular policy applies. For example, it could be that the hypothetical policy on unofficial software is intended to apply only to the organization's own on-site resources and employees and not to contractors with offices at other locations. Additionally, the policy's applicability to employees travelling among different sites and/or working at home who need to transport and use disks at multiple sites might need to be clarified.

Module 3, Chapter 2

Roles and Responsibilities. The assignment of roles and responsibilities is also usually included in issue-specific policies. For example, if the policy permits unofficial software privately owned by employees to be used at work with the appropriate approvals, then the approval authority granting such permission would need to be stated. (Policy would stipulate, who, by position, has such authority.) Likewise, it would need to be clarified who would be responsible for ensuring that only approved software is used on organizational computer resources and, perhaps, for monitoring users in regard to the use of unofficial software.

Compliance. For some types of policy, it may be appropriate to describe, in some detail, the infractions that are unacceptable, and the consequences of such behaviour. Penalties may be explicitly stated and should be consistent with organizational personnel policies and practices. When used, they should be coordinated with appropriate officials and offices and, perhaps, employee unions. It may also be desirable to task a specific office within the organization to monitor compliance.

Points of Contact. For any issue-specific policy, the appropriate individuals in the organization to contact for further information, guidance, and compliance should be indicated. Since positions tend to change less often than the people occupying them, specific positions may be preferable as the point of contact. For example, for some issues the point of contact might be a line manager; for other issues it might be a facility manager, technical support person, system administrator, or security program representative. Using the above example once more, employees would need to know whether the point of contact for questions and procedural information would be their immediate superior, a system administrator, or a computer security official.

Areas Appropriate for Issue-specific Policies

Some of the areas in which management today needs to consider issue-specific IT security policies are covered in this section. These topics are intended to be illustrative rather than exhaustive. Although many of these topics are standard to any discussion of IT security, an organization would necessarily need to tailor its policies relating to them to meet its own unique needs.

Physical security: The physical protection of and access to IT resources and facilities will generally need to be addressed in one or more specific policies. In organizations with extensive IT systems and equipment, this may mean developing policies that address such issues as who has access to what sites/locations; how often risks to installations are analyzed and by whom; what types of physical access controls and monitoring equipment are put in place; what responsibilities will be assigned to

trained security officials and what activities and responsibilities will be required of all employees.

Personnel Security: Depending on the types of activities being performed, degree of data sensitivity to be encountered, and number of personnel, specific security policies related to personnel screening, requirements, hiring, training, evaluating, and firing may need to be developed and administered. It may be appropriate that a trained personnel security specialist initiate, review, approve, and perform all security-related personnel actions.

Communications Security: Communications security is a complex technical specialty unto itself. In organizations where day-to-day business relies on communicating routinely with remote locations, the security of the communications transmissions and lines is usually an issue that needs to be addressed by policy. If the data being transmitted is highly sensitive, then this concern is magnified, and issue-specific security policies may need to be developed on a number of activities. Issues associated with the use of cryptography and its related options and procedures, the use of modems and dial-in lines, and precautions against wiretapping are just some of the potential issues to be addressed.

Administrative Security: Administrative security as it applies to IT system management and oversight activities comprises many potential security policy issues. Included are such topics as input/output controls, training and awareness, security certification/accreditation, incident reporting, system configurations and change controls, and system documentation.

Risk Management: Risk management involves assessing IT resources in terms of potential threats and vulnerabilities and planning the means for counteracting those identified risks. Issues that will need to be addressed by policies include how, by whom, and when the assessments should be performed; and what type of documentation should result.

Contingency Planning: Related to Risk Management, Contingency Planning means planning for the emergency actions to be taken in the event of damage, failure, and/or other disabling events that could occur to systems. Issues that need to be addressed by policies include determining which systems are most critical and therefore of highest priority in contingency planning; how the plans will be tested, how often, and by whom; and who will be responsible for approving the plans.

Examples of Issue-Specific Policies

Identity Management Policies

- ▶ **Account/Password Authentication:** A unique account and password combination must authenticate all users of information systems. The

Module 3, Chapter 2

account name must be used only by a single individual, and the password must be a secret known only to that individual.

- ▶ **Account Changes:** The manager responsible for the end user must request changes in access privileges for corporate information systems for a system account. End users may not request access-privilege changes to their own accounts. The request must be recorded and logged for the record.
- ▶ **New Account Requests:** The manager responsible for a new end user must request access to corporate information systems via a new account. End users may not request their own accounts. The new account request must be recorded and logged for the record. When the account is no longer needed, the account must be disabled.
- ▶ **Login Message:** All computer systems that connect to the network must display a message before connecting the user to the network. The intent of the login message is to remind users that information stored on company information systems belongs to the company and should not be considered private or personal. The message must also direct users to the corporate information system usage policy for more detailed information. The message must state that by logging on, the user agrees to abide by the terms of the usage policy. Continuing to use the system indicates the user's agreement to adhere to the policy.
- ▶ **Failed Login Account Disabling:** After five successive failed login attempts, a system account must be automatically disabled to reduce the risk of unauthorized access. Any legitimate user whose account has been disabled in this manner may have it reactivated by providing both proof of identity and management approval for reactivation.
- ▶ **Employee Account Lifetime:** Permanent employee system accounts will remain valid for a period of 12 months, unless otherwise requested by the employee's manager. The maximum limit on the requested lifetime of the account is 24 months. After the lifetime of the account has expired, it can be reactivated for the same length of time upon presentation of both proof of identity and management approval for reactivation.

Network Policies

- ▶ **Extranet Connection Access Control:** All extranet connections (connections to and from other companies' networks outside of the corporation, either originating from the external company's remote network into the internal network, or originating from the internal network going out to the external company's remote network) must limit external access to only those services authorized for the remote company. This access control must be enforced by IP address and TCP/

UDP port filtering on the network equipment used to establish the connection.

- ▶ **System Communication Ports:** Systems communicating with other systems on the local network must be restricted only to authorized communication ports. Communication ports for services not in use by operational software must be blocked by firewalls or router filters.
- ▶ **Unauthorized Internet Access Blocking:** All users must be automatically blocked from accessing Internet sites identified as inappropriate for company use. This access restriction must be enforced by automated software that is updated frequently.
- ▶ **Virtual Private Network and Dial-Up:** All remote access to the corporate network is to be provided by virtual private network (VPN) or direct landline connections. Dial-up access into the corporate network is not allowed.

Data Privacy Policies

- ▶ **Copyright Notice:** All information owned by the company and considered intellectual property, whether written, printed, or stored as data, must be labeled with a copyright notice in the following format: Copyright © 2003 [Company Name], Inc. All Rights Reserved
- ▶ **E-mail Monitoring:** All e-mail must be monitored for the following activity:
 - ▼ Non-business use
 - ▼ Inflammatory, unethical, or illegal content
 - ▼ Disclosure of company confidential information
 - ▼ Large file attachments or message sizes
- ▶ **Customer Information Sharing:** Corporate customer information may not be shared with outside companies or individuals.
- ▶ **Encryption of Data Backups:** All data backups must be encrypted.
- ▶ **Encryption of Extranet Connection:** All extranet connections must use encryption to protect the privacy of the information traversing the network.
- ▶ **Data Access:** Access to corporate information, hard copy, and electronic data is restricted to individuals with a need to know for a legitimate business reason. Each individual is granted access only to those corporate information resources required for them to perform their job functions.

Data Integrity Policies

- ▶ **Virus-Signature Updating:** Virus signatures must be updated immediately when they are made available from the vendor.
- ▶ **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- ▶ **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.

Module 3, Chapter 2

- ▶ **Version Zero Software:** Version zero software (1.0, 2.0, and so on) must be avoided whenever possible to avoid undiscovered bugs.
- ▶ **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.
- ▶ **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
- ▶ **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

System Administration Policies

- ▶ **Application Monitoring:** All servers containing applications designated for monitoring must be constantly monitored during the hours the application operates. At least the following activities must be monitored:
 - ▼ Application up/down status
 - ▼ Resource usage
 - ▼ Non-standard behaviour of application
 - ▼ Addition or change of the version, or application of software patches

- Intrusion-Detection Monitoring:** All critical servers must be constantly monitored at all times for intrusion detection. This monitoring must cover at least the following categories:
- ▼ Port scans and attempts to discover active services
 - ▼ Non-standard application connections
 - ▼ Non-standard application behaviour
 - ▼ Multiple applications
 - ▼ Sequential activation of multiple applications
 - ▼ Multiple failed system login attempts
- ▶ **Firewall Monitoring:** All firewalls must be constantly monitored, 24x7, by trained security analysts. This monitoring must include at least the following activities:
 - ▼ Penetration detection (on the firewall)
 - ▼ Attack detection (through the firewall)
 - ▼ Denial of service detection
 - ▼ Virus detection
 - ▼ Attack prediction
 - ▼ Penetration blocking
 - ▼ Attack blocking
 - ▼ Virus blocking
 - ▼ Intrusion response
- ▶ **Network Security Monitoring:** All internal and external networks must be constantly monitored, 24x7, by trained security analysts. This monitoring must detect at least the following activities:

- ▼ Unauthorized access attempts on firewalls, systems, and network devices
- ▼ Port scanning
- ▼ System intrusion originating from a protected system behind a firewall
- ▼ System intrusion originating from outside the firewall
- ▼ Network intrusion
- ▼ Unauthorized modem dial-in usage
- ▼ Unauthorized modem dial-out usage
- ▼ Denial of services
- ▼ Correlation between events on the internal network and the Internet

Usage Policies

- ▶ **Personal Use of Information Systems:** Personal use of company computer systems may be allowed on a limited basis to employees provided that it does not interfere with the company's business, expose the company to liability or damage, compromise the company's intellectual property, or violate any laws. Employees should be advised that the company may at any time be required by law to print or copy files, e-mail, hard copy, or backups and provide this information to government or law enforcement agencies.
- ▶ **Personal Use of Telephones:** Corporate phone systems may be used for limited, local, personal calls, as long as this usage does not interfere with the performance of the corporate business.

Physical Security Policies

- ▶ **Room Access Based on Job Function:** Room access must be restricted based on employee job function.
- ▶ **Position of Computer Monitors:** Computer monitors must be faced away from windows to discourage "eavesdropping."
- ▶ **Badges on Company Premises:** All corporate employees on the controlled premises must display badges with picture identification in plain view.

System-Specific Policy

Program policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. System-specific policy fills this need. It is much more focused, since it addresses only one system.

Many security policy decisions may apply only at the system level and may vary from system to system within the same organization. While these decisions may appear to be too detailed to be policy, they can be

Module 3, Chapter 2

extremely important, with significant impacts on system usage and security.

These types of decisions can be made by a management official, not by a technical system administrator. The impacts of these decisions, however, are often analyzed by technical system administrators.

To develop a cohesive and comprehensive set of security policies, officials may use a management process that derives security rules from security goals. It is helpful to consider a two-level model for system security policy: security objectives and operational security rules, which together comprise the system-specific policy. Closely linked and often difficult to distinguish, however, is the implementation of the policy in technology.

Security Objectives

The first step in the management process is to define security objectives for the specific system. Although, this process may start with an analysis of the need for integrity, availability, and confidentiality, it should not stop there. A security objective needs to be more specific; it should be concrete and well defined. It also should be stated so that it is clear that the objective is achievable. This process will also draw upon other applicable organization policies. Security objectives consist of a series of statements that describe meaningful actions about explicit resources. These objectives should be based on system functional or mission requirements, but should state the security actions that support the requirements.

Development of system-specific policy will require management to make trade-offs, since it is unlikely that all desired security objectives will be able to be fully met. Management will face cost, operational, technical, and other constraints.

Operational Security Rules

After management determines the security objectives, the rules for operating a system can be laid out, for example, to define authorized and unauthorized modification. The rules specify who (by job category, organization placement, or name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions.

The degree of specificity needed for operational security rules varies greatly. Generally, the more detailed the rules are, the easier it is to know when one has been violated. At the same time, it is also, easier to automate policy enforcement. However, inordinately detailed rules may make the job of instructing a computer to implement them difficult or computationally complex.

In addition to deciding the level of detail, management should decide the degree of formality in documenting the system-specific policy. Once

again, the more formal the documentation, the easier it is to enforce and to follow policy. On the other hand, policy at the system level that is too detailed and formal can also be an administrative burden. In general, good practice suggests a reasonably detailed formal statement of the access privileges for a system. Documenting access controls policy will make it substantially easier to follow and to enforce. Another area that normally requires a detailed and formal statement is the assignment of security responsibilities. Other areas that should be addressed are the rules for system usage and the consequences of non-compliance.

Policy decisions in other areas of security, are often documented in the risk analysis, accreditation statements, or procedural manuals. However, any controversial, atypical, or uncommon policies will also need formal statements. Atypical policies would include any areas where the system policy is different from organizational policy or from normal practice within the organization, either more or less stringent. The documentation for a typical policy contains a statement explaining the reason for deviation from the organization's standard policy.

Example of System-Specific Policies: Payroll System

- ▶ **Security Objectives:** Only individuals in the accounting and personnel departments are authorized to provide or modify information used in payroll processing.
- ▶ **Operational Security Rule:** Personnel clerks may update fields for weekly attendance, charges to annual leave, employee addresses, and telephone numbers. Personnel specialists may update salary information. No employees may update their own records.

Policy Implementation

Policy implementation is a process. Policy cannot merely be pronounced by upper management in a one-time statement or directive with high expectations of its being readily accepted and acted upon. Rather, just as formulating and drafting policy involves a process, implementation similarly involves a process, which begins with the formal issuance of policy.

Policy Documentation

Once security policy has been approved and issued, it may be initially publicized through memorandums, presentations, staff meetings, or a variety of means. As soon as possible, though, it will also need to be incorporated into formal policy documentation as well. The process of documenting policies will usually require updating existing documentation as well as creating new documentation.

Existing Documentation: Information security will need to be integrated into many existing activities and practices throughout many levels of the organization. This integration will be facilitated by revising any existing

Module 3, Chapter 2

applicable documentation to reflect new procedures, rules, and requirements. Included may be the modification of various existing documents, forms, and plans at all levels of the organization to reflect the policy.

For example, if IT equipment purchases and/or upgrades have been reviewed and approved based on documented criteria such as cost, productivity, maintainability, etc., then security considerations may need to be introduced into that criteria. Also, if it has previously been the documented policy to review the progress and status of internal IT systems under development, then security-related concerns should be introduced into that review process.

New Documentation: Additionally, the development of many new documents, such as guidelines, standards, and procedures, may be required. This is often true in large organizations performing many different activities and having many levels of management. In such environments, different functional elements may have widely differing IT systems and needs to accommodate. It is therefore generally more practical, to the extent possible, to allow elements to tailor their implementations of policy to meet their unique needs. This can be accomplished through the development of documents containing more detailed procedures and practices to be used for specific kinds of systems and activities within functional elements.

For example, organizations will want to issue policies to decrease the likelihood of data loss due to technology failures and/or operator errors. A program-level policy might state something to the effect that: "It is the policy of the organization to ensure against data loss due to accidents or mishaps." In an area where extensive writing and editing of lengthy documents is performed, such as a word processing or technical publications unit, security documentation might be developed on saving work in-progress much more often than would usually be done, and/or utilizing automatic "save" features on IT systems and software. In a different type of functional area, however, where, for example, databases are maintained that do not undergo significant changes very often, the security documentation might focus on procedures for the database administrator to use in performing periodic (daily, weekly, etc.) backups of the system.

Policy Visibility

Policies are generally public documents, however in many cases parts of the policies may be kept private. High visibility should be afforded to the formal issuance of the information security policy. This is due to a combination of factors, including the following:

- ▶ Nearly all employees at all levels will in some way be affected;
- ▶ Major organizational resources are being addressed;
- ▶ Many new terms, procedures, and activities will be introduced.

Information security policy should be afforded visibility through such avenues as management presentations, discussions, question/answer forums, and newsletters can be beneficial, as resources permit. Including information security as a regular topic at staff meetings at all levels of the organization can also be a helpful tactic. As an aspect of providing visibility for security policies, information should also be included regarding the applicable high level directives and requirements to which the organization is responding. Educating employees as to the requirements specified by the various laws and related regulations will help emphasize the significance and timeliness of computer security, and it will help provide a rational basis for the introduction of information security policies.

Visibility should be afforded the information security policy through all applicable documentation. The more integral security policy is to all other aspects of daily routines, the more quickly the associated actions and practices will become natural to doing business. Ultimately, among the goals of policy are the assimilation of a common body of knowledge and values and the demonstration of appropriate corresponding behaviours. Those goals will be expedited by making the information security policy integral to the organization through all avenues.

System-Specific Policy Implementation

Technology plays an important but not sole role in enforcing system-specific policies. When technology is used to enforce policy, it is important not to neglect non-technology-based methods. For example, technical system-based controls could be used to limit the printing of confidential reports to a particular printer. However, corresponding physical security measures would also have to be in place to limit access to the printer output or the desired security objective would not be achieved.

Technical methods frequently used to implement system-security policy are likely to include the use of logical access controls. However, there are other automated means of enforcing or supporting security policy that typically supplement logical access controls. For example, technology can be used to block telephone users from calling certain numbers. Intrusion detection software can alert system administrators to suspicious activity or can take action to stop the activity. Personal computers can be configured to prevent booting from a floppy disk. Technology-based enforcement of system-security policy has both advantages and disadvantages. A computer system, properly designed, programmed, installed, configured, and maintained, consistently enforces policy within the computer system, although no computer can force users to follow all procedures. Management controls also play an important role and should not be neglected. In addition, deviations from the policy may sometimes be necessary and appropriate; such deviations may be dif-

Module 3, Chapter 2

difficult to implement easily with some technical controls. This situation occurs frequently if implementation of the security policy is too rigid (which can occur when the system analysts fail to anticipate contingencies and prepare for them).

Interdependencies

Information Security Policy is related to many other areas:

Program Management. Policy is used to establish an organization's computer security program, and is therefore closely tied to program management and administration. Both program and system-specific policy may be established in any area. For example, an organization may wish to have a consistent approach to incident handling for all its systems and would issue appropriate program policy to do so. On the other hand, it may decide that its applications are sufficiently independent of each other that application managers should deal with incidents on an individual basis.

Access Controls. System-specific policy is often implemented through the use of access controls. For example, it may be a policy decision that only two individuals in an organization are authorized to run a check-printing program. Access controls are used by the system to implement (or enforce) this policy.

Other Areas. Information security policy can be related to nearly every topic covered in this course material on some level. This is because all of the topics discussed in the material have associated issues that organizations may need to address via policies. The topics most directly related, however, are: security program management and administration; personnel; security training and awareness; contingency planning; and physical and environmental security.

Awareness, Training and Education

People, who are all fallible, are usually recognized as one of the weakest links in securing systems. The purpose of computer security awareness, training, and education is to enhance security by:

- ▶ improving awareness of the need to protect system resources;
- ▶ developing skills and knowledge so computer users can perform their jobs more securely; and
- ▶ building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Making computer system users aware of their security responsibilities and teaching them correct practices helps users change their behaviour. It also supports individual accountability, which is one of the most important ways to improve computer security. Without knowing the nec-

essary security measures (and to how to use them), users cannot be truly accountable for their actions.

Cost Considerations

A number of potential costs are associated with developing and implementing computer security policies. Overall, the major cost of policy is the cost of implementing the policy and its impacts upon the organization. Establishing an information security program, accomplished through policy, does not come at negligible cost.

Other costs may be those incurred through the policy development process. Numerous administrative and management activities may be required for drafting, reviewing, coordinating, clearing, disseminating, and publicizing policies. In many organizations, successful policy implementation may require additional staffing and training and can take time. In general, the costs to an organization for computer security policy development and implementation will depend upon how extensive the change needed to achieve a level of risk acceptable to management.

Audit of IS Security Policy

Standards such as ISO 17799, provide benchmarks for reviewing security policies. Security policies are reviewed for three broad purposes- benchmarking against external standards, due to changes in the risk perception, and due to implementation of new information system within the firm. Given below is an illustrative checklist relating to audit of IS Security Policy:

- ▶ Whether a well-documented security policy is available?
- ▶ Whether Inventory of IT assets is made part of the policy?
- ▶ Whether policies related to IT activities are listed in the security policy?
- ▶ Whether the policy takes into account the business strategy for the next 3 - 5 years?
- ▶ Whether the policy takes into account the legal requirements?
- ▶ Whether the policy takes into account the regulatory requirements?
- ▶ Whether the policy is approved and adopted by the Board of Directors / Senior Management?
- ▶ Whether the policy is communicated to all concerned and is understood by them?
- ▶ Whether the following major security areas are covered in the policy?
 - ▼ PC and LAN, MAN and WAN security
 - ▼ Physical Security to IS establishments
 - ▼ Handling of confidential information
 - ▼ Handling of security incidents
 - ▼ Privacy related issues for outside entities
 - ▼ E-mail security

Module 3, Chapter 2

- ▼ Application security
- ▼ Interface Security
- ▼ Password Security
- ▼ Operating system security, web site security
- ▼ Database security
- ▼ Anti virus and piracy policy
- ▼ Archived and Backed up data security
- ▼ Procedures for handling incidence of security breach
- ▼ Disaster Recovery Plan
- ▼ Use of cryptology and related security
- ▶ Persons responsible for implementing security policy and consequence for wilful violation of the Security Policy
- ▶ Whether a review process is in place for reviewing the policy at periodic intervals and / or on any other major event?

Summary

The term “information security policy” generally refers to important information asset and computer security related decisions taken by the management. There are three basic types of policies, Program policy, Issue-specific policies, and system-specific policies. A computer security program policy is a strategic document used to create an organization’s computer security program. Issue-specific policies, as the name implies, address specific issues of concern to the organization. System-specific policies focus on decisions taken by management to protect a particular system.

Since the policy is written at a high level, most organizations also develop standards, guidelines and procedures that offer users, managers, and others the details necessary to implement the policy. Policies and other supporting documents are highly structured documents that have a format that is usually consistent organisation-wide.

Policies are ineffective unless implemented. Apart from documenting the policy, management must undertake a training exercise in order to inculcate desirable security procedures and practices. Technology plays a significant role in enforcing policies, however non-technical methods are also effective in many situations.



3 Logical Access Controls

✂ Learning Goals ✂

To understand:

- ▶ The Objectives of Logical Access
- ▶ The Paths of Logical Access
- ▶ Logical Access Exposures
- ▶ Authentication Techniques
- ▶ Operating System Security
- ▶ Database Security

Introduction

In order to compromise a system, the first hurdle that the attacker must cross is to be able to connect to the system and its data. There are many ways to prevent people from accessing the data stored within a system, but in any organisation it is necessary to allow certain people to connect and to disallow others. The most commonly adopted strategy is to insist on proof of identity, thus limiting access only to known users and to limit each user's activity to certain operations. These twin controls are Authentication and Authorisation. In this chapter, we look at various ways that data can be accessed and how authentication and authorisation can help ensure that only the right person access the right data.

Objectives of Logical Access

Securing logical access to information assets, addresses two primary objectives:

- ▶ **Securing resident data:** Significant volumes of data resides in computing equipment and devices.
- ▶ **Securing data in transit:** Much of data is also in transit between computers or between networks, travelling on communication channels, which are susceptible to a wide range of risks. This deals with securing data travelling on networks and security of the network itself.

However, data does not exist independently. Securing data therefore implies the securing information resident in computing equipment or storage media and transiting communication channels and devices may include any/all of the following:

- ▶ **Information, Data:** Includes Database (master and transaction files), data repositories, correspondence files, spreadsheets, backups and archives.

Module 3, Chapter 3

- ▶ **Application Software:** Includes business critical applications such as Sales, Purchases, Inventory, Production control and office automation software.
- ▶ **Systems Software:** Includes operating systems, network management software, systems utilities, communications software, compilers, access control software.
- ▶ **System and data Components:** data dictionaries, data directories, log files, access control lists, temporary transaction files, job schedule lists, spool, and procedure libraries.

The purpose of information security is to protect the confidentiality, integrity and availability of information. These security objectives in turn imply the following:

- ▶ Information should be protected from being accessed by unauthorized persons/processes and authorized persons/processes who/which do not have specific right of access thereto.
- ▶ However, in a commercial environment access to information should not be unduly restrictive as it will have a negative impact on employee and efficiency.
- ▶ Information should be protected from unauthorized modification by persons or processes, which adversely affect the completeness, accuracy and validity of information.

Paths of Logical Access

Gaining logical access requires access to some computing equipment, device, storage media or communication channel, which is directly or indirectly connected to the desired computer or IS resource.

Some common modes of logical access are given below:

Mainframe Terminals: Access to the mainframe central computer can be obtained through any of the dumb or intelligent terminals connected to the central computer, which contains the data, applications and systems software. Such terminals are usually capable of minimal functions such as data entry, querying, running minimal applications etc.

Console: One or some terminals connected to the mainframe are configured for privileged access capable of commanding and controlling the functions and operations of the central computer and attached devices.

Networked Computer: Access to a computer or resources on the network can be enabled by simply connecting a computer to the network. This is a very broad category which includes computer connecting to a secured network as a trusted computer thus giving unrestricted access to the secure network, a computer housing the middleware system which has trusted connection with the other back end components of the network, a backup server.

Client/Server: The client server technology offers distinct advantages over the central server concept enabling distributed computing. In client/server one of the computers connected to the network can function as the server and any other as the client but are also capable of switching roles. Hence the information and processing tends to get distributed across locations and computing equipment on the network, thus raising the concerns of multiple points of access.

Three-tier and N-tier Systems: When three-tier or N-tier systems are involved, network access becomes very complex. Users may access the network from a middle tier, in which case only the middle tier may be known to the database; the individual user's authorizations may be lost. To ensure confidentiality, the database must be able to identify the actual user who is accessing it from the middle tier.

Networked Devices: Access to resources on a computer or network can also be achieved through telecommunication devices which provide for access paths such as hubs, switches and routers, point of sale device, wireless equipment.

Dial-Up Access: Users located at a remote location can dial-up the organisation's server using public or private telecommunication lines and gain access to organisational data.

Logical Access Exposures

Technical Exposures

Improper logical access can result in loss or damage to information and information resources leading to undesirable consequences for an organisation. Improper logical access results in a violation of the confidentiality or integrity or availability of information. Some of the technical exposures relating to logical access are discussed as follows:

Data Leakage: Information in electronic form is highly susceptible to leakage and stealing. Sensitive information contained in computer files may be copied on to disks or other media, electronically transferred across networks to other locations, transmitted across the Internet or simply viewed or printed. Even accidentally, users may be able to lay hands on sensitive information contained in the systems, due to improper logical access security.

Wire Tapping: This is similar to tapping of telephone lines, networking cables or telecommunication lines are tapped by the perpetrator for eavesdropping. This can also be accomplished by use of special probes without any damage to the communication media.

Scavenging or Dumpster Diving: The perpetrator gains access to apparently inconspicuous directories or areas such as recycle bins, temporary files,

Module 3, Chapter 3

deleted files, redundant configuration settings. This can be used by the perpetrator to put together critical information about the organisation or subject of attack.

Emanation Interception: Many of the devices used for computing radiate signals or waves, such as electromagnetic radiation emanated by dot matrix printers and monitors, which can be intercepted using simple devices.

Data Diddling: This is possibly the least technical of the various logical Issues and exposures. This involves unauthorized modification of input submitted for processing. This could simply involve manually altering the information on the input documents such as vouchers or invoices awaiting to be entered or as they are entered. This also includes modification of information containing in electronic form such as input files or transaction files, awaiting processing.

Piggybacking: The perpetrator waits for the authorised user to log into the system and leave it unattended. The perpetrator may then be in a position to carry out any activity that the authorised user was permitted to do.

Masquerading: A perpetrator impersonates as the legitimate user thereby gaining access to the system or information contained therein. A perpetrator, posing as a legitimate user, sends a message to the Systems Administrator telling him that the user (perpetrator) has lost his password and leads the systems administrator to allot a new password, which is then used for gaining wrongful access to the system. In another kind of masquerading attack, the perpetrator sends a message to all users requiring them to shut their systems or disclosing some sensitive information, deceiving the users into believing that the message is coming from an authorised user.

Spoofing: The perpetrator uses IP spoofing to convince a system that it is communicating with a known trusted entity in order to provide the intruder with access to the system. IP spoofing involves the alteration of TCP packet, by inserting a source address of a known and trusted host instead of the attacker's host. The target may accept the packet and act up on it leading to undesirable consequences.

Asynchronous Attacks: Such attacks are specific to devices, which exchange data asynchronously. In asynchronous transmission, the sender and the receiver do not operate at the same speed, hence the data is often stored in temporary buffers awaiting transmission or processing. Such data which are waiting for transmission, are susceptible to attacks, wherein a perpetrator uses a pin-like insertions into the buffer to tap data stored in the buffer. Asynchronous attacks are often complex and difficult to detect.

Keystroke monitoring (also called Key Logging): Keystroke monitoring is a process whereby system administrators view or record both the keystrokes entered by a computer user and the computer's response during a user-to-computer session. Examples of keystroke monitoring would include viewing or capturing characters as they are typed by users, reading users' electronic mail, and viewing other recorded information typed by users. It is also used as a diagnostic in software development to determine sources of error in computer systems. Such systems are also highly useful for law enforcement, eavesdropping, and espionage – for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures. Keystroke monitoring can be achieved by both hardware and software means. Commercially available systems include devices which are attached to the keyboard cable (and thus visible if the user makes a thorough inspection) and also devices which can be installed in keyboards (thus invisible to users).

Buffer Overflow: A program or process can receive more data than it can handle. If the developer has not written the instructions on how the process should behave when handling excessive data, the program may malfunction. This malfunction can be exploited by a malicious attacker.

Rounding Down: The perpetrator rounds down the amounts in various transactions to the nearest desired decimal place. This involves small modifications to the transaction values whereby the rounded difference is routed to a pre-designated account. A perpetrator can induce the bank transaction processing system to alter the value of clearing credits to various customer accounts from say Rs.5,45,859.37 rounded down to Rs.5,45,859.35 and transfer Rs.0.02 to an unauthorized account.

Salami Technique: This is similar to the Rounding Down technique except that in this case the perpetrator slices off a fixed value from each amount. For example, a perpetrator can modify a program that calculates interest to account holders, in such a way that, a small fixed amount, say Rs. 0.03, is deducted from all payments and transferred to an unauthorized account.

Trap Doors: Trap doors are application system vulnerabilities which allow the perpetrator to bypass security protections and allows him to insert unauthorized logic or modify the behaviour of application systems in undesirable ways. Usually, a trapdoor is created by the original programmer to allow him access to the system.

Remote Shut Down: The perpetrator uses various techniques to assess the vulnerabilities and loopholes of a system and attempts to gain access to the operating system. She then remotely and maliciously shuts down the system causing a loss of system availability and perhaps loss of integrity as the data may be corrupted during the unplanned shut down.

Module 3, Chapter 3

Denial of Service (DoS): The perpetrator attempts to flood memory buffers and communication ports to prevent delivery of normal services. This and the more aggressive Distributed Denial of Service attack are dealt with in a subsequent chapter.

Social Engineering: The perpetrator uses social and tactical skills to obtain information such as passwords, PIN etc. exploiting the human weaknesses of greed, appeasement and fear.

Malicious Code

Malicious code (also called “Malware”) is the name used for any program that adds to, deletes or modifies legitimate software for the purpose of intentionally causing disruption and harm or to circumvent or subvert the existing system’s function. Examples of malicious code include viruses, worms, Trojan Horses, and logic bombs. Newer malicious code is based on Active X and Java applets.

Viruses: Viruses are a type of malicious code that attaches to a host program and propagates when an infected program is executed. Such code may be programmed to play mere pranks or cause severe damage. The perpetrator’s objective is to multiply and spread the code. However viruses are dependent on another program or human action to replicate or to activate their payload. Viruses are not capable of self-actuating.

Worms: Worms are malicious programs that attack a network by moving from device to device. However worms differ from viruses in that for replication or activation of code, they do not depend on any program or human action but are self-actuating and self-sustaining. Hence worms spread much more rapidly than viruses.

Trojan Horses: Trojan horses hide malicious code inside a host program that seems to do something useful. Once these programs are executed, the malicious code hidden in the Trojan horse program is released to attack the workstation, server, or network or to allow unauthorized access to those devices. Some Trojans are programmed to open specific ports to allow access for exploitation. Then the open Trojan port could be scanned and located, enabling an attacker to compromise the system. Trojans are common tools used to create backdoors into the network for later exploitation by crackers.

Logic Bombs: Logic bombs are often legitimate programs, to which malicious code has been added. Their destructive action is programmed to “blow up” on meeting a logical event such as time or logical event as number of users, memory/disk space usage, etc. Every time the infected program is run, the logic bomb checks external environment to see whether the condition to trigger the bomb has been met. If not, control is passed back to the main application and the logic bomb waits. If the

condition is satisfied, the rest of the logic bomb's code is executed, and it attacks the system. Logic bombs are very difficult to detect since they reside in the system and its destructive instruction set is known only after it blows up.

Macro Viruses: Macro viruses are the most prevalent computer viruses, accounting for the vast majority of virus encounters. A macro virus can easily infect many types of applications, such as Microsoft Excel and Word. To infect the system, macro viruses attach themselves to the application's initialization sequence (often stored in a template file), and then when the application is executed, the virus's instructions execute before control is given to the application. Then the virus replicates itself, infecting more and more of the system. These macro viruses move from system to system through email file sharing, data sharing, and disk sharing. Today's widespread sharing of macro-enabled files, primarily through email attachments, has rapidly increased the threat from macro viruses.

Polymorphic Viruses: Polymorphic viruses are difficult to detect because they hide themselves from antivirus software by altering their appearance after each infection. Some polymorphic viruses can assume over two billion different identities.

Stealth Viruses: Stealth viruses attempt to hide their presence from both the operating system and the antivirus software by encrypting themselves. They are similar to polymorphic viruses in that they are very hard to detect.

Adware and Spyware: These are often software that tracks the Internet activities of the user usually for the purpose of sending targeted advertisements. Besides the loss of privacy and waste of bandwidth (loss of availability), they do not pose other security related risks, as yet. However, it is quite likely that Trojans could be embedded in such software. Adware and Spyware often come with some commercial software, both packaged as well as shareware software. There is often a reference to the Adware and Spyware software in the license agreement.

Controls over Malicious Code

The best control for malicious code is preventive. An organisation should have sound policies and procedure in place that prevent such undesirable software in the first place. The second line of defence against such malicious software are Ant-Virus software and Anti-Adware and Anti-spyware software.

Policy and Procedural Controls

- ▶ The Security Policy should address virus threats, systems vulnerabilities and controls. A separate section on Anti-virus is appropriate to address the various degree of risks and suitable controls thereof.
- ▶ The installation of software that contains Adware and Spyware must be forbidden by the security policy.
- ▶ Anti-virus awareness and training on symptoms of attacks, methods of reducing damage, cleaning, quarantining should be given to all employees.
- ▶ Hardware installations and associated computing devices should be periodically verified for parameter settings.
- ▶ As part of SDLC, there should be controls to ensure that development area is free of viruses and sufficient safeguards are in place to secure the area from viruses.
- ▶ Provision of drives to read media should be restricted only to controlled terminals.
- ▶ Network access to the Internet should be restricted and monitored.
- ▶ The servers and all terminals should have network based anti-virus software installed with sufficient number of user licences.
- ▶ Procedures should ensure systematic updates are applied to all anti-virus installations at frequent intervals.
- ▶ The use of external media such as disks, CDs, tapes, etc. should be prevented. If necessary such media should be scanned on a stand-alone machine and certified by the IS Department.
- ▶ Vendors and consultants should not be allowed to run their demonstrations and presentations on organisational systems.
- ▶ All new software acquisitions should follow a controlled procedure of centralized acquisition and testing for viruses.
- ▶ Patches to operating systems and other software, upgrades thereof should be acquired from authentic sources and scanned before installation.
- ▶ Reporting and incident handling procedures should be in place to suitably handle virus incidents and eradicate them at the earliest.
- ▶ The organization should implement and monitor an effective backup plan and ensure back-up media are not infected and is preferably encrypted and that only new media are used for back-up purposes.

The predominant technical control over malicious code is anti-virus software. Anti-virus software can be broadly defined as software that detects, prevents and in some cases removes malicious and other unwanted software. An anti-virus software has three components:

- ▶ **Scanners:** The software looks for a sequence of bits called virus signatures that are characteristic of virus codes. They check memory, disk boot sectors, executables, systems files to find matching bit patterns. In this context it may be noted that over 1500 new viruses emerge

every month. Hence it is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.

- ▶ **Active Monitor and Heuristic Scanner:** This component looks for critical interrupt calls and critical operating systems functions such as OS calls, BIOS calls, which resemble virus action. However this also makes them inefficient since they cannot differentiate between genuine systems calls and virus action. These could result in false alarms.
- ▶ **Integrity Checkers:** Integrity checkers can detect any unauthorized changes to files on the system. This requires the software to “take stock” of all files resident on the system and compute a binary check data called as the Cyclic Redundancy check. When a program is called for execution, the software computes the CRC again and checks with the parameter stored on the disk. However such checks assume that frequent changes to applications and systems utilities do not occur.

Further technical controls such as securing systems with hardware based password and encryption locks, remote booting are also used. However there is no single control which acts as a panacea guaranteeing against virus attacks; rather virus control is a combination of management, technical, administrative, application and importantly operational controls. Note that to detect and remove Adware and Spyware, there are commercially available Anti-Adware and Anti-Spyware software.

Access Controls and Authentication

The process of access control involves the following steps:

- ▶ Identification of the user seeking access. Identification is a process by which a user provides a claimed identity to the system such as an account number.
- ▶ Authentication of the user. Authentication is a mechanism through which the user's claim is verified.
- ▶ Authorising the user for a pre-determined set of actions on eligible resources or also referred to as action privileges.
- ▶ Accounting for use of resources by the user and actions performed

Of the above, implementing the right authentication is the most challenging. Authentication is the process of verifying that the identity claimed by the user is actually true. There are three ways in which a user can be authenticated. There are

- ▶ Based on what the user knows, i.e. information to be remembered by the user.
- ▶ Based on what the user has, i.e. device or token in the possession of the user
- ▶ Based on what the user is, i.e. physical characteristics of the user.

In a high security installation, all the three factors may be combined to provide what is called three-factor authentication.

Authentication Techniques

As stated above, authentication may be through remembered information, possessed tokens, or physical characteristics. We shall examine each class of authentication techniques below.

Passwords and PINs

This is the most common authentication technique that depend on remembered information. The user, initially, identifies himself using his login-id to the system and then provides the password information. Once the system is able to get match is successful for the both fields, the system authenticates the user and enables access to resources based on the authorization matrix. However if a match is not successful, the systems returns a message (such as “Invalid User or password”) thus preventing access to resources.

Personal Identification Numbers (PINs) are a type of password, usually a 4-digit numeric value that is used in certain systems to gain access, and authenticate. The PIN should be such that a person or computer cannot guess it in sufficient time by using a guess and check method, i.e. where it guesses the PIN, and checks for correctness by testing it on the system that the person is attempting to gain access to and the processes repeated with a different guess till access is obtained. PINs are most often used for gaining access to Automatic Teller Machines(ATMs).

Weaknesses of Logon mechanism

Logon/password access security is based on information to be remembered by the user (what the user knows). This results in the following weaknesses:

- ▶ Passwords are easily shared. Users often advertently or inadvertently reveal passwords leading to security being compromised.
- ▶ Repeated use of same password could lead to passwords being easily guessed by others.
- ▶ If a password is too short or too easy, the chances of the password being guessed are quite high.
- ▶ If a password is too long or too complex, the user may forget or may write it down.
- ▶ If many applications have to be accessed by one user, many passwords have to be remembered.
- ▶ Passwords can be shared, guessed, spoofed or captured.

Recommended practices for strong passwords

- ▶ The user should not share the authentication information viz. password.

- ▶ The password should be easy for the user to remember but hard for the perpetrator to guess.
- ▶ On creation of a new user, the first password is allotted by the security administrator and a change of password is forced on the first login.
- ▶ Users should be encouraged or forced to change passwords periodically e.g. once in 60 days.
- ▶ Concurrent logins by same user should not be permitted.
- ▶ Passwords should not be too short and should not use name of user, pet, common words found in dictionary or such other attributes. Password combination should be random and use alphabetic, numeric and special characters(such as “!”, “#”, “^”, etc.).
- ▶ Passwords should be changed periodically.
- ▶ Number of wrong login tries should be restricted to three, after which the system should lockout the user. Further access can be granted only through the intervention of the security administrator.
- ▶ The logon ids active in the system should not exceed the number of users actually authorised to access systems resources.
- ▶ Passwords should be stored in an encrypted form using one-way encryption.
- ▶ In case the a user remains inactive at a terminal, for a length of time (say 20 minutes), the terminals should lock out the user and require the user to login again.

Attacks on logon/password systems

Due to their inherent weaknesses, logon-id/password access control technique is vulnerable to various kinds of malicious attacks. Some of the common attacks on such systems are discussed below:

- ▶ **Brute force:** In this crude form of attack, the attacker tries out every possible combination to hit on the successful match. The attacker may also use various password cracking software that assist in this effort.
- ▶ **Dictionary attack:** On the similar lines as brute force, this type of attack is based on the assumption that users tend to use common words as passwords, which can be found in a dictionary, hence the name. The “dictionary” simply consists of a list of words, including proper names (Raju, Ramesh, Ibrahim, etc) and also that of mythological or religious figures (Krishna, Jesus, Osiris, Buddha, etc.).
- ▶ **Trojan:** As discussed elsewhere in this material, a Trojan is a malicious software, which the attacker can use to steal access control lists, passwords or other information.
- ▶ **Spoofing attacks:** In this technique, the attacker plants a Trojan program, which masquerades as the system’s logon screen, gets the logon and password information and returns control to the genuine

Module 3, Chapter 3

access control mechanism. Once the information is obtained, the attacker uses the information to gain access to the system resources.

- ▶ **Piggybacking:** As stated earlier, an unauthorized user may wait for an authorised user to log in and leave a terminal unattended. The logical techniques that are used to secure against this attack are to automatically log out the session after a pre-determined period of inactivity or by using password-protected screen savers.

Token Based Authentication

Objects that a user is required to possess for identification and authentication are known as tokens.

Plastic Cards: Plastic cards contain information about the user and primarily provide a means of identification of the user and can enable authentication. Plastic cards can further be of the following types:

- ▶ **Memory tokens:** In its most common form, the cards contain visible information such as name, identification number, photograph and such other information about the user and also a magnetic strip. This magnetic strip stores static information about the user. In order to gain access to a system, the user in possession of a memory token may be required to swipe his card through a card reader, which reads the information on the magnetic strip and passes onto the computer for verification with stored information to enable access. e.g. Employee badges with encoded magnetic strips. Where two-factor authentication is adopted, the user is not only required to have his card read by a card reading device but also required to key in a remembered information (passwords, PIN) to gain access to the system resources. e.g. Bank ATM Card.
- ▶ **Smart Tokens:** In this case, the card or device contains a small processor chip which enables storing dynamic information on the card. Besides static information about the user, the smart tokens can store dynamic information such as bank balance, credit limits etc.,. However the loss of such smart cards can have more serious implications.

Proximity Readers: In this case when a person in possession of the card reaches the restricted access area, the card data is read by the proximity readers (or sensors) which transmits information to the authentication computer, which enable access to the restricted area or system. The advantages are that the user is not required to insert the card into the device hence access time is faster. Proximity tokens can be either static or processor based. In static tokens, the card contains a bar code, which has to be brought in proximity of the reader device. In case of processor based tokens, the token device, once in the range of the reader, senses the reader and transmits a series of codes to the reader.

Other token based systems include challenge response systems and one time passwords, these have been dealt with in the chapter on Network Security.

Single Sign-on: Single sign-on is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The single sign-on, which is requested at the initiation of the session, authenticates the user to access all the applications they have been given the rights to on the server, and eliminates future authentication prompts when the user switches applications during that particular session.

In many organisational situations, one user, by virtue of his job responsibilities is often required to log into more than one applications. This raises the complex issue of multiple logon and passwords, for the user to remember. This is often solved by a single sign-on, which enables user access to various applications entitled for access. However this often requires transferring all login control to an access control system, careful configuration of authorities, strong passwords and adequate security of password information since compromise of a single login giving access to multiple applications can lead to many systems being compromised. Single Sign on can be run either from the user's workstation or from a central server. However the concern in a decentralized processing or database environment is that the passwords travel over communication lines.

Biometric Security

Biometrics offers a very high level of authentication based on "what the user is", as compared to logon and token based authentication. Biometrics as the name suggests is based on certain physical characteristics or behavioural patterns identified with the individual, which are measurable. The International Biometric Group defines biometrics as automated mechanism which uses physiological and behavioural characteristics to determine or verify identity and further explains that the physiological biometrics are based on measurements and data derived from direct measurement of a part of the human body. Behavioural biometrics are based on measurements and data derived from an action and indirectly measure characteristics of the human body Based on some feature unique to every user, biometrics seek to minimize the weaknesses in other mechanisms of authentication. Some of the biometric characteristics which are used are:

- ▶ Fingerprint
- ▶ Facial Scan
- ▶ Hand Geometry
- ▶ Signature
- ▶ Voice

Module 3, Chapter 3

- Keystroke Dynamics
- Iris Scanners
- Retina Scanners

Implementation of biometric authentication is often expensive and involves the following phases:

- Identification of IS assets which require biometric security
- Based on the above, identification of appropriate biometric application
- Acquisition and Testing of appropriate hardware, calibration of error rates for effectiveness and efficiency of enrolment and readability
- Implementation of administrative procedures for exception reporting and adjustment for false positives
- Enrolment of Users
- Implementation of related physical and logical controls

Identification and authentication is based on a match with items in the database containing data captured during the user enrolment. Registration or enrolment of the individuals' physical or behavioural characteristics involves capture of information, digitizing and storage of the biometric data. Based on the data read by the sensor, the image or digitized data is compared to the stored data to obtain a match. If the match succeeds, authentication is successful.

However due to the complexity of data, biometrics suffer from two types of error viz. False Rejection Rate (FRR) which is wrongfully rejecting a rightful user and False Acceptance Rate (FAR) which involves an unauthorized user being wrongfully authenticated as a right user. Ideally a system should have a low false rejection and low false acceptance rate. Most biometric systems have sensitivity levels which can be tuned. Generally speaking, the more sensitive a system becomes, FAR drops while FRR increases. Thus, FRR and FAR tends to inversely related. An overall metric used is the Crossover Error Rate (CER) which is the point at which FRR equals FAR.

Due to their complexity and high cost of implementation, biometric access controls were initially implemented only for high value critical information resources such a defence, banking etc. However with the rapid decrease in the cost of biometric hardware and stabilization in error rates, biometrics are being increasingly preferred for commercial applications. Finger print based biometrics are quite popular and widely deployed in data centres.

Cost-Benefit Analysis

The need for, or value of any particular authentication technique must be weighed against the its costs, resource drain and its usefulness. Any organisation can choose to have a very secure system, but there is al-

ways a point of diminishing returns. Excessive security can not only be expensive, but can even detract from the business function. A formal cost-benefit analysis, supported by evidence and documentation must be carried out before any of these authentication mechanisms are adopted.

Access Controls in Operating Systems

Operating systems presents security challenges that are different from those in more general application programs. Operating system (and databases) must provide different access to different items by different kinds of users. Operating system developers must pay careful attention to defining access, granting access and controlling intentional and unintentional corruption of data and relationships. The means of achieving them are discussed below.

Security Kernel

A kernel (also called a nucleus or core) is the part of an operating system that performs the lowest-level functions. In standard operating system design, the kernel implements operations such as synchronization, inter-process communication, message passing, and interrupt handling.

A security kernel is responsible for enforcing the security mechanisms of the entire operating system. The security kernel provides the security interfaces among the hardware, operating system, and other parts of the computing system and stores, encrypts and controls access to password files and other authentication related data. Typically, the operating system is designed so that the security kernel is contained within the operating system kernel.

There are several good design reasons why security functions are isolated in a security kernel.

- ▶ **Coverage.** Every access to a protected object must pass through the security kernel. In a system designed in this way, the operating system can use the security kernel to ensure that every access is checked.
- ▶ **Separation.** Isolating security mechanisms both from the rest of the operating system and from the user space makes it easier to protect those mechanisms from penetration by the operating system or the users.
- ▶ **Unity.** All security functions are performed by a single set of code, so it is easier to trace the cause of any problems that arise with these functions.
- ▶ **Modifiability.** Changes to the security mechanisms are easier to make and easier to test.
- ▶ **Compactness.** Because it performs only security functions, the security kernel is likely to be relatively small.

Module 3, Chapter 3

- ▶ **Verifiability.** Being relatively small, the security kernel can be analyzed rigorously. For example, formal methods can be used to ensure that all security situations have been covered by the design.

On the other hand, implementing a security kernel may degrade system performance because the kernel adds yet another layer of interface between user programs and operating system resources. Moreover, the presence of a kernel does not guarantee that it contains all security functions or that it has been implemented correctly. And in some cases a security kernel can be quite large.

Reference Monitor

The most important part of a security kernel is the reference monitor, the portion that controls accesses to objects. A reference monitor is not necessarily a single piece of software, it is the collection of access controls for devices, files, memory, inter-process communication, and other kinds of objects. It is an object that maintains the access control policy. It does not actually change the access control information; it only provides information about the policy.

The security reference monitor is a separable module that enforces access control decisions and security processes for the operating system. All security operations are routed through the reference monitor, which decides if the specific operation should be permitted or denied. Thus, a reference monitor acts like a wall around the operating system or trusted software.

The main elements of an effective reference monitor are that it is:

- ▶ **Always on:** Security must be implemented consistently and at all times for the entire system, for every file and object.
- ▶ **Not subject to preemption:** Nothing should be able to pre-empt the reference monitor. If this were not the case, then it would be possible for an entity to bypass the mechanism and violate the policy that must be enforced.
- ▶ **Tamperproof:** It must be impossible for an attacker to attack the access mediation mechanism such that the required access checks are not performed and authorizations not enforced.
- ▶ **Lightweight:** It must be small enough to be subject to analysis and tests, to prove its effectiveness.

A reference monitor can control access effectively only if it cannot be modified or circumvented by a rogue process, and it is the single point through which all access requests must pass. Furthermore, the reference monitor must function correctly if it is to fulfil its crucial role in enforcing security. Because the likelihood of correct behaviour decreases as the complexity and size of a program increase, the best assurance of

correct policy enforcement is to build a small, simple, understandable reference monitor.

The reference monitor is not the only security mechanism of a trusted operating system. Other parts of the security suite include audit, identification, and authentication processing, as well as the setting of enforcement parameters, such as who the allowable subjects are and what objects they are allowed to access. These other security parts interact with the reference monitor, receiving data from the reference monitor or providing it with the data it needs to operate.

Pluggable Authentication Modules

While passwords are the most dominant form of authentication, several alternatives like token-based authentication and biometrics are in existence. Many of the operating systems provide interfaces that allow third-party authentication system to handle the authentication. In some operating systems (notably, Linux and Solaris) these interfaces are provided via Pluggable Authentication Modules (PAM). PAM provides a way to develop programs that are independent of authentication scheme. These programs need “authentication modules” to be attached to them at runtime in order to work. Which authentication module is to be attached is dependent upon the local system setup and is at the discretion of the local system administrator. PAMs also provide facilities for authentication management, account management, session management and password management. PAM also enables the Single Sign On mechanism.

When used correctly, PAM provides the following advantages for a system administrator:

- ▶ It provides a common authentication scheme that can be used with a wide variety of applications.
- ▶ It allows great flexibility and control over authentication for both the system administrator and application developer.
- ▶ It allows application developers to develop their program without implementing a particular authentication scheme. Instead, they can focus purely on the details of their program.

File permissions

In most operating systems, every file is owned by a user and can be accessed by its owner, group or public, depending upon access permissions. When a user creates a file or directory, that user becomes the default owner of that file or directory. A user may be member of one group or many groups. Further, a user owner of a file may not be part of the group that also may have access to the file. Again, most operating systems have at least three types of file permissions; read, write and execute. The users have to be given at least read access to many of the system files.

Access Control Lists (ACL)

An access control list is a table that tells the computer operating system which access rights each user has to a particular system object, such as a directory/folder or an individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Most of the major operating systems use access control lists, though the list is implemented differently by each operating system. But in whatever form it is implemented, it is the foundation of any security functionality.

Access control enables one to protect a system or part of the system (directories, files, file types, etc.). When the system receives a request, it determines access by consulting a hierarchy of rules in the ACL. ACL has one or more access control entries (ACEs), each consisting of the name of a user or a group of users. The user can also be a role name, such as programmer or tester. For each of these users, groups, or roles, the access privileges are stated in a string of bits called an access mask. Generally, the system, administrator or the object owner creates the access control list for an object.

Identity Management

The latest development in access control is called Identity Management. These are services and solutions which provide an organisation with an integrated enterprise-wide authentication system(s). They help an organisation to distribute and manage the identities of staff, partners and clients who need controlled access to sensitive business information, so that an organisation can be sure that each user really is who they claim to be. These systems manage the roll-out, operation and revocation of passwords, tokens, biometrics or other authentication credentials to an organisation's users.

DAC vs. MAC

Access control lists can be further refined into both required and optional settings. This is more precisely carried out with discretionary access control and is implemented by discretionary access control lists (DACs). The difference between discretionary access control (DAC) and its counterpart mandatory access control is that DAC provides an entity or object with access privileges it can pass to other entities.

Mandatory access control (MAC) requires that access control policy decisions be beyond the control of the individual owners of an object. MAC is generally used in systems that require a very high level of security. With MAC, it is only the administrator and not the owner of the re-

source that may make decisions that bear on or derive from the security policy. Only an administrator may change the category of a resource, and no one may grant a right of access that is explicitly forbidden in the access control policy. MAC is always prohibitive (i.e., all that is not expressly permitted is forbidden), and not permissive.

Operating System Security Evaluation: The Common Criteria

System consumers are generally not security experts. While there is a need for security functions, the users are not usually capable of verifying the accuracy or adequacy security functions. Thus it has become necessary for independent third party evaluation of operating system security. Over the years, several of the advanced nations independently developed schemes for such evaluation. Sometime in the early 1990s the International Organization for Standardization (ISO) began to develop a new set of standard evaluation criteria for general use that could be used internationally. The new methodology is now called the Common Criteria. The goal was to unite the various international and diverse standards into new criteria for the evaluation of information technology products. This effort ultimately led to the development of the Common Criteria, now an international standard in ISO 15408:1999. Common Criteria version 2.1 is the current version of the Common Criteria. The Common Criteria can be freely downloaded from <http://www.common-criteriportal.org>

Chinese Wall Security Policy

The Chinese Wall Security Policy reflects certain commercial needs for information access protection. The security requirements reflect issues relevant to those people in legal, medical, investment, or accounting firms who might be subject to conflict of interest. A conflict of interest exists when a person in one company can obtain sensitive information about people, products, or services in competing companies.

The security policy builds on three levels of abstraction.

- ▶ **Objects.** At the lowest level are elementary objects, such as files. Each file contains information concerning only one company.
- ▶ **Company groups.** At the next level, all objects concerning a particular company are grouped together.
- ▶ **Conflict classes.** At the highest level, all groups of objects for competing companies are clustered.

With this model, each object belongs to a unique company group, and each company group is contained in a unique conflict class. A conflict class may contain one or more company groups. For example, suppose there is an auditing firm with clients in several fields: automobiles, banks, and airlines. The firm might want to store data on automotive companies Bajaj and TVS; on banks Stanchart, SBI (State Bank of India),

Module 3, Chapter 3

and IOB (Indian Overseas Bank); and on airlines, Jet Airways. Using the Chinese Wall hierarchy, the firm would form six company groups (one for each company) and three conflict classes: {Bajaj, TVS}, {Stanchart, SBI, IOB}, and {Jet Airways}.

The hierarchy guides a simple access control policy: A person can access any information as long as that person has never accessed information from a different company in the same conflict class. That is, access is allowed if either the object requested is in the same company group as an object that has previously been accessed or the object requested belongs to a conflict class that has never before been accessed. In the example given, initially one can access any of the objects. Suppose an auditor reads from a file on Bajaj. A subsequent request for access to any bank or to Jet Airways would be granted, but a request to access TVS files would be denied. The next access, say, of Jet Airways data, does not affect future accesses. But if the auditor then access a file on SBI, that person will be blocked from future accesses to Stanchart or IOB. From that point on, one can access objects only concerning Bajaj, Jet Airways, SBI, or a newly defined conflict class.

The Chinese Wall is a commercially inspired confidentiality policy. It is unlike most other commercial policies, which focus on integrity. It should be noted that access permissions change dynamically: As a subject accesses some objects, other objects that would previously have been accessible are subsequently denied.

Database Security

At a superficial level, access control for a database appears to be similar to access control for operating systems or any other component of a computing system. However, access control in a database is more complicated. Operating system objects, such as files, are unrelated items, whereas records, fields, and elements are related. Although a user cannot determine the contents of one file by reading others, a user might be able to determine one data element just by reading others. The problem of obtaining data values from others is called **INFERENCE**.

It is important to notice that you can access data by inference without needing direct access to the secure object itself. Restricting inference may mean prohibiting certain paths to prevent possible inferences. However, restricting access to control inference also limits queries from users who do not intend unauthorized access to values. Moreover, attempts to check requested accesses for possible unacceptable inferences may actually degrade the DBMS's performance.

Database Roles and Permissions

Databases are very useful because they centralize the storage and maintenance of data. This means that limited access is both a responsibility

and a benefit of this centralization. Databases are often separated logically by user access privileges. The database administrator specifies who should be allowed access to which data, at the view, relation, field, record, or even element level. The DBMS must enforce this policy, granting access to all specified data or no access where prohibited. Furthermore, the number of modes of access can be many. A user or program may have the right to read, change, delete, or append to a value, add or delete entire fields or records, or reorganize the entire database.

The general process of access control begins with specifying to which database(s) a login may connect. Then, permissions must be assigned within the database. Generally, database administrators will create “groups” or “roles,” and each of these will contain users. Specific permissions are assigned to the roles. This process is quite similar to the practices that are suggested for modern network operating systems. Additionally, some relational database platforms allow groups to be nested, thereby allowing you to create a hierarchy of permissions.

For example, a database administrator might create a role that allows Sales Staff to insert and update data in a specific table. Users of this role might also be able to call certain stored procedures, views, and other database objects. Another role might be created for Sales Managers. This role may be provided with the ability to delete sales-related data and make other changes within the database. Through the use of roles, database administrators can easily control which users have which permissions. Note, however, that it is very important to properly design security based on the needs of database users. Again, the principal of providing the least required permissions should be kept in mind. This is especially important since, through the use of the SQL language, well-meaning users can accidentally delete or modify data when their permissions are too lax.

Views

Perhaps the most commonly used method of controlling data access is views. A view is a logical relational database object that actually refers to one or more underlying database tables. Views are generally defined simply as the result of a (SQL) query. This query, in turn, can pull information from many different tables and can also perform common calculations on the data.

Although views provide many advantages to database developers, they can also be very valuable from a security standpoint. First, views provide database administrators with a method to define granular permissions settings that would not otherwise be possible. For example, one can create a view that shows basic information about employees, but that excludes sensitive data like their salaries and medical details. Or, one could

Module 3, Chapter 3

define a view that allows users to see data for only particular employees within the company (for example, only the employees they manage).

Once a view has been defined, one can assign object-level permissions to the view. Users of the database can then use the view to access whatever information they require. If at a later point of time, changes in security area required, one can simply change the definition of the view itself, and all authorized users will be able to see this value in their result set. Furthermore, views can query other views, thereby creating a chain of objects based on business rules. When portions of the logic change, only some of the views may be affected. And, if business or technical requirements change, corresponding changes in the view can be made.

Views are generally used to return sets of data to users. Database developers can even allow users to modify data through the use of views, in a controlled manner.

Stored Procedures

Database logic can become significantly complex, and common operations often must be performed by many different users. Database servers offer developers the ability to create and reuse SQL code through the use of objects called stored procedures. Stored procedures can be used to perform any function that is possible through the use of standard SQL commands. Additionally, they can take arguments, making them very flexible.

For example, a stored procedure might be used to automatically perform common operations on a set of customer-related database tables. When a customer record changes, corresponding changes can be easily made by calling the stored procedure. Related to security, and like views, instead of giving direct access to modify data stored in base tables (which in some cases might be too liberal, or your users may not completely understand how to modify the data), you can give access to stored procedures. This provides a layer of abstraction between the underlying database tables that might be affected and allows for encapsulating many of users' most common operations in manageable code modules.

Triggers

Triggers are designed to automatically be “fired” whenever specification actions take place within a database. For example, a developer can create a trigger on a “SalesOrder” table that will automatically create a corresponding row in the Invoice table. Triggers can also be used to perform complex data validation. An example would be one that checks to ensure that certain transactions are entered only at the end of a financial period.

From a security standpoint, triggers can be used in different ways. First, triggers can be used to perform detailed auditing. For example, whenever a change is made to certain information in an “EmployeeSalary” table, you might want to notify a high-level manager, or you might write a row logging this action to another table. Another use of triggers is to enforce complex database-related rules. For example, to ensure that a series of actions is always taken when data changes are made, an appropriate trigger can do the job.

Database Restrictions

One of the important objectives of access controls is to prevent any threats to the integrity and unauthorized access to the database resources. Relational Database works on the principles of tables and relations and allows rules of integrity and access to be specified. The principle of least privileges to data items can be enforced using views as against reads. Such rules can be restricted by a range of parameters such as permissible values or limits, operations upto the granularity of a data field etc.

Restrictions can also be implemented at schema level based on the following:

- ▶ **Name-Dependent:** Users access to a data resource is restricted based on their action privileges with respect to the data resource i.e. only users are allowed action privileges based on the name of the data resource. For example, a payroll clerk is allowed to view all the data fields, except that related to, say employee’s medical history.
- ▶ **Content Dependent:** Access to resources can also be based on contents being queried/accessed. Where the access to a user is restricted to a particular degree of sensitivity of resources, user is not allowed to access content of higher degree of sensitivity. A petty cashier is not allowed access to transactions with value in excess of a prescribed limit.
- ▶ **Context Dependent:** Using diverse queries, a user may be able to infer about content permissible only for higher access security. In order to secure against such improper access, access is restricted to all contextual references to data with higher security. E.g. Even though a user may not have access to income data of customers, he may query the database and obtain a list of customer making high value purchases, which allows him to infer the income of the customer.
- ▶ **History Dependent:** Sometimes a user may construct a series of queries in such a way that each query and its answer does not violate the security policy, but taken together the answer to all the queries would given her information to which she is not authorised.

In addition to views and triggers, restrictions can also be technically applied using menu based controls. That is access to data and action privi-

leges can be restricted using well structured menus and restricting access to menu options based on category of user.

Audit Trail

An Audit Trail is a record to enable the reconstruction and examination of the sequence of events of a transaction, from its inception to the output of final results or from output to the events and transactions. Audit trails maintain a record of system activity, both by computer systems and users. Audit trails assist in detection of security violation, segregation of duties, etc. Audit trails are maintained at various levels – operating systems, network component, application and database. Audit trail maintained at the OS and Network component level is generally called logs, or more specifically **SYSTEM-LEVEL LOGS**. The audit trail maintained at application level is called an **APPLICATION LEVEL LOG**. For complete reconstruction of the scenario both should be maintained. Application level audit trail augments the system level log by logging user activities including specific action done at the data level.

Audit of Access Controls

Some of the factors critical to the successful achievement of audit objectives with regard to evaluating logical access are:

- ▶ The understanding of an organisation's information security framework, security policy linkage of IT objectives to its business objectives and assessment of risk and controls. This often forms the foundation for risk management and criteria for determining the amount of investment and philosophy of access controls.
- ▶ Selection and implementation of appropriate access controls should be consistent with the organisation's structure, management controls and organisational culture.
- ▶ Top management's commitment, support and control must be communicated to all levels in the organisation and concerned stakeholders. Management support would be evident from the emphasis and investment on training and education of users, the importance given to access controls and the enforcement of access control discipline.
- ▶ Management controls should be evaluated to determine if adequate systems are in place. This also helps to detect, report and take corrective action on access security violation.
- ▶ The auditor's opinion depends on his understanding of general and IS controls and audit procedures. These are used to test the effectiveness and efficiency of access to organisational information, in respect of which the auditor should exercise due care and diligence.

Review of risk management

The IS auditor should plan his work so as to meet the audit objectives well before conducting the audit of logical security. AAS 8 (ICAI) on Audit Planning, requires that the auditor as a preliminary step also ob-

tain an understanding of audit environment and risk management practices of the client. Some of the steps to achieve this objective are outlined in the following paragraphs.

Understand the business and technical infrastructure of the organisation processes

The auditor should understand the client's business controls and complex significance and materiality of IS resources, the types of events, transactions and practices that significantly impact logical access controls. AAS 20 (ICAI) on Knowledge of Business, prescribes the outline on the extent of knowledge about business that an auditor should obtain, not only while taking up the audit assignment for the first time but also changes to the understanding already gained, due to changes in the business environment.

One of the primary and critical objectives of instituting a system of information systems audit is to ensure continuing protection of organisational assets. In this direction, the IS auditor should determine whether the organisation has a dynamic risk assessment and management process and resource classification and then test the adequacy of controls to protect against risks.

The organisation should have procedures and mechanisms to ensure that the risks from compromise of logical access paths should be assessed on a periodic basis and on the happening of significant events. For example, purchase of a modem by departments having access to the core nation-wide network exposes the entire network to threats from open networking, if the modem is used on any of the network workstations.

The independent review of risks and risk assessment process in the organisation, enables the IS auditor to gain an understanding of the material risks that arise from a logical perspective.

From the perspective of logical security, even small changes in the business process leading to changes in the IS process can lead to significant logical security issues. For e.g. an organisation may be working on a highly secure closed network. However, enabling even a remote workstation on the network to the Internet access can compromise the entire resources on the network. This is because it opens up a logical path to the closed network.

The auditor should exercise special care while gaining preliminary understanding of networked computing environment. For this he should review the network diagrams mapping both physical and logical networks.

Inventory

An important requirement of risk management is that there should be continuous inventory verification of all information resources and assets. Each asset should be identified with respect to its value and criticality vis-à-vis various factors prominently effect access controls. Appropriate risk rating and investment in access security can be decided based on this valuation. This is an iterative process since changes in any components in a network could have the potential to compromise access security of an application or components elsewhere in the network.

Identification of data owner

Once the various components of information assets are identified and classified, owners for each of components and their users should be determined. This is an important step in fixing accountability for the protection of the asset and responsibilities thereto.

In order to reduce his audit risk and for conduct of efficient audit, the auditor should in consultation with the management, determine materiality thresholds with respect to classification of resources and users, risk ranking. The Audit and Assurance Standard on Audit Materiality (AAS-13) provides that the auditor should consider materiality and its relationship to audit risk when conducting audits.

The IS auditor should besides understanding the extent of computerisation of business processes and activities, give special consideration to critical processes and unusual transactions.

Based on the above factors, the levels of materiality should be established to meet the audit objectives.

The auditor can gain preliminary information on access controls by studying the security policy and procedures, interviewing personnel, especially those assigned with responsibilities for protecting logical access such as the security administrator, data and database administrators, operations managers and users. The understanding of security requirements with respect to various IS resources is critical for planning the nature and extent of audit procedures.

Audit Procedures - Special Considerations

The objective and scope of audit would determine the audit procedures and IS resources to be covered. Often evaluation of logical access controls forms a part of a generic IS audit covering various other controls. However, the auditor may be required to evaluate the logical access security of a system, sub- system, application, operating software, database management software and the like.

Identification of logical access paths

An auditor has to identify the possible access paths permitting access to information resources. He must document the logical paths and prescribe appropriate audit procedures to evaluate every component in the information systems infrastructure to enable identification of logical access paths. This is often a challenging and complex task when it comes to auditing in networking computing environments. Identification and documentation of access paths involves testing security at various layers:

Hardware: This includes computer workstations, terminal devices, communication devices, peripherals etc. constituting the physical interface with the users. Physical security of hardware forms a critical and inseparable component of information security, which works in tandem with logical security and other category of controls. Successful implementation of security policy often lies in the fine orchestration of various controls to achieve the objectives of information security in an organisation. Here the auditor should have special consideration for covert channels and communications devices (e.g. modems, network interface cards) connected to computers.

Systems software: The command and control of hardware rests in the proper implementation of operating systems and other systems software. Hardware works in tandem with, and its operation is synchronised by, systems software which forms the foundation for effective systems security. From a logical perspective, a wrong setting of systems level parameters can compromise the security of the application and other systems software, which talk to the systems software. Besides, firmware and systems software often enforce the first level access control including logon and password security. Systems with communication facilities enable sharing of resources but present higher level of risks, hence the IS auditor should take special care to ascertain which devices are connected and provided with communication capabilities. He would need to evaluate the management standards and implementations of network access controls.

Database Management System: In environments involving voluminous data handling, a Database Management System (DBMS) manages the organisation of data in the databases. The auditor is required to evaluate the access security enforced by the DBMS, which could include relational databases, schema definitions, access to data dictionary, directory services and scripts to restrict access implemented by the DBMS.

Application software: Application software represents the business logic, which interfaces with the user and business process requirement, from the user perspective. The auditor focuses on the effectiveness of bound-

Module 3, Chapter 3

ary controls and other input, processing and output controls, discussed elsewhere in this module.

Access control software: The auditor may also encounter situations with networked environments and with users having access to various applications. In such cases user and program access to applications and IS resources to numerous applications are controlled by an access control software. The auditor should evaluate the access permissions configured in the software and ascertain their appropriateness to the organisation's functional requirements.

In the above cases, the assessment of state of access controls can be quite technical, presenting complexities for the IS auditor. Therefore, in cases, where the controls involve technical sophistication, the auditor has to rely on the services of a technical expert, who possesses special skills, knowledge and experience in the particular field. Where the auditor relies on the work of an expert, he should evaluate the work and the extent of reliance on the work of the expert. Attention in this regard is also invited to AAS 9 on "Using the work of an Expert". The auditor's report should explicitly state this fact of IS auditor's reliance on work of other experts.

Audit Test Procedures

IS auditors should evaluate whether logical access policies and procedures are effectively implemented. For this the auditor has to test if:

- ▶ Necessary access control framework in the form of logical access security policies and standards are in place and effectively communicated. This the auditor does by studying the various policies, the system of communication of policy initiatives and the system of education and training users with respect to logical security of information resources. The auditor would need to interview data owners, users and custodians to evaluate their knowledge and skills on implementation of access controls.
- ▶ Procedures and mechanisms for logical access are implemented to ensure protection of organisational information. The IS auditor should evaluate the various logical security techniques and mechanisms for their effective implementation, operation and administration.
- ▶ The auditor must check if the controls are functioning effectively and efficiently. This requires the auditor to conduct various compliance and substantive tests to determine if the logical security of information resources is actually effective. The auditor can determine the level of effectiveness of logical security by determining compliance with procedure manuals such as administrator manuals and user manuals, interviewing users and administrators and testing the

various logical security mechanisms to determine any weaknesses or incompatibilities.

Some audit considerations in this regard are outlined below:

Systems Configuration

Test the appropriateness of system configuration and parameter settings. Appropriate configurations of access security parameter systems while installing/ upgrading hardware, software such as operating systems, systems software, DBMS and application software are critical in building a strong foundation for access security. In this respect the auditor would have to evaluate whether:

- ▶ The system configuration complies with the organisational security standards, security policy requirements, manufacturer specifications and best practices for security.
- ▶ There is a process to ensure that configuration of access security settings and parameters and changes thereto are authorised, documented and tested.
- ▶ Adequate security is in place for boot up and fault tolerance.
- ▶ Privileged and special purpose logons are controlled and documented.
- ▶ There is a procedure for control over purchase, custody and management of system utilities. Many systems utilities are powerful and can break through the various levels of access security.

Logical Access mechanisms

Testing of various logical access mechanisms such as token based authentication systems, and biometric access control systems. The auditor can conduct tests that determine:

- ▶ The control of authorisation, custody, operation and termination over use of tokens such as badges, memory and smart cards.
- ▶ Control over special terminals and devices. For instance, a hub may be exposed physically but with proper levels of encryption, logical security of information can be ensured.
- ▶ Security practices with respect to unattended terminals, security of data in transit and control over production resources.
- ▶ Whether logging of transactions and events is appropriately enabled.

User account management and password management

Logon and passwords are the most commonly used mechanisms to secure logical access to information resources. The auditor should:

- ▶ Evaluate mechanisms such as access control features and software to identify weaknesses if any.
- ▶ Evaluate the effectiveness of user management procedures through audit of access control lists to assess if access is permitted based on the principle of least privileges and “need to know-need to do” basis,

Module 3, Chapter 3

scan audit logs to determine the effectiveness of access control and interview users, and identify all entries in ACL with the authorised list of employees permitted to access systems.

- ▶ Test user profiles and group profiles to determine the access privileges and controls thereon.

Privileged logons and special user accounts

Privileged logons and special user accounts provide higher level of access to systems resources. Hence, they require a higher levels of access security and management. The auditor should evaluate:

- ▶ The strength of controls on such privileged access. He should follow appropriate audit procedures to identify all individuals having access to such privileged logon facility and special user accounts. The auditor should critically evaluate the need for such access
- ▶ Review audit trails, access violation reports in respect of all privileged logons and special user accounts
- ▶ The strength and adequacy of monitoring and incident handling procedures

Access to file directories and application logic and system instruction sets

The auditor should evaluate the protection of:

- ▶ Systems files and directories containing critical hardware and systems software configuration and parameter files such as driver information, etc.
- ▶ Application files and directories containing application programs, support files, program libraries, parameter files, initialisation files, etc.
- ▶ Production data and directories containing production files and production resources.

Monitoring and reporting procedures

Besides testing preventive controls, the auditor should also ensure that there are adequate systems and procedures for monitoring and reporting incidents involving security violations. In evaluating the adequacy of such controls, he should evaluate if:

- ▶ Management controls are in place with personnel designated with responsibilities for security management and administration.
- ▶ Appropriate security events are logged and reported.
- ▶ Audit log files and information are adequately backed up and protected from access.
- ▶ Systems are in place to report security incidents and process violations.

- ▶ Appropriate reports are produced to summarise the data recorded in audit logs so that security events may be efficiently monitored on a timely basis.
- ▶ Appropriate and timely action on critical changes in security requirements is taken to implement/modify appropriate controls to meet newly identified risks.

Bypass Security Procedures

There may be various situations in the routine course of operations where security features are bypassed for operational and functional convenience during certain controlled operations. For instance, privileged logons may be provided to systems engineers to meet emergency situations, bypass label processing may be provided to meet certain bulk processing requirements or systems exits may be enabled during software implementation and maintenance phases. The auditor should identify all such provisions and critically audit the events.

Appendix: Logical Access Controls Checklist

The following is an illustrative questionnaire that could be used to review Logical Access Controls within operating systems and databases

User Account Maintenance

- ▶ Each and every user ID in the operating system level should have been created only after specific approval of the concerned manager in writing on a request form signed by the respective user. Verify whether such approval is in place for all the active user IDs.
- ▶ Apart from the approved request forms, there should be a user profile record with details such as, Employee Name, Designation, Employee Number, Date of joining, User ID allotted, Date of creation of user ID, Date of deletion of user ID, Signature of the user, Authoriser, etc. Verify whether the above mentioned register is maintained. All the entries in the register should be accounted for in the list of active user IDs obtained from the operating system.
- ▶ Check that with the exception of reserved user accounts created for the internal use of the operating system, RDBMS, Application system, etc., all other user accounts are uniquely identifiable by the respective user's personal name. In other words, generic user accounts, which cannot be attributed to any individual, should not be allowed. Verify this and comment.
- ▶ Check the operating system user IDs which have security equivalence to super user/root user and ensure whether they are permissible as per management guidelines.
- ▶ Check whether all the user IDs are protected with passwords.
- ▶ Ensure whether all default vendor accounts (with the exception of super/root user) shipped with the operating system have been disabled. This should be checked after each upgrade or installation.

Module 3, Chapter 3

- ▶ Check the list of active user groups and ensure that general users are not members of sensitive / privileged user groups which have higher privileges.

Logical Access Controls

- ▶ Ensure that access to operating system command prompt is disabled for general users.
- ▶ If some or more of the system administration related activities are driven through a menu-based utility assigned to any user ID, which is privileged, ensure that such ID(s) cannot be used to bypass login security and access the command prompt.
- ▶ Ensure that the file pertaining to each user containing login parameters cannot be modified by the respective user.
- ▶ Ensure that no modification can be done to the system activity log file.
- ▶ Check whether access rights to system files, application executable program files, application data files, utilities, application parameter files, system/database configuration/initialization files, etc. have been adequately controlled to allow read / write / execute / modify, etc. as the case may be to appropriately authorised users on need to know, need to do basis.
- ▶ Obtain a list of world writable (accessible to every user) directories / folders in the system and ensure that they have been set only in accordance with management guidelines.
- ▶ Verify the access rights settings for the users' home directories and ensure that they are not owned by any ID other than the actual user. Also, ensure that user's home directory cannot be accessed by any other user.

System Administration

- ▶ Ensure that the facility to logon as super/root user is restricted to system console for security reasons.
- ▶ Check the password definition parameters included in system and ensure that minimum password length is specified according to the security policy of the organisation.
- ▶ Ensure that the maximum validity period of password is not beyond the number of days permitted in the security policy.
- ▶ Check whether the parameters to control the maximum number of invalid logon attempts has been specified properly in the system according to the security policy.
- ▶ Check whether password history maintenance has been enabled in the system to disallow same passwords from being used again and again on rotation basis.
- ▶ Verify if the parameters to control the password format has been properly set according to security policy.

- Verify the parameters in the system to control automatic log-on from a remote system and ensure whether they have been properly set according to security policy.
- Verify the parameters in the system to control the number of concurrent connections a user can have and ensure that it is restricted as per security policy.
- Examine the terminal inactive time allowable for users and verify if the time set is in accordance with the guidelines.
- Check whether automatic logging of user activities is enabled.
- Check for users logged on to the system at odd times (midnight, holidays, etc).

Maintenance of sensitive user accounts

- Ascertain as to who is the custodian of sensitive passwords such as super/root user and verify if s/he is maintaining secrecy of the password, whether she has preserved the password in a sealed envelope with movement records for usage in case of emergency.
- From the log file, identify the instances of use of sensitive passwords such as super user and verify if records have been maintained with reason for the same. Ensure that such instances have been approved/authorised by the management.
- From the log file, identify the instances of unsuccessful logon attempts to super user account and check the terminal ID / IP address from which it is happening. Check if appropriate reporting and escalation procedures are in place for such violations.

Database Controls: Physical access and protection

- Is there a list of databases with the names of administrators?
- Does IT Department identify and segregate hardware hosting these databases?
- Whether there is a clear partition between application area and data areas within the system?
- Does the IT Department have a laid down standards / conventions for database creation, storage, naming and archival?
- Are database administrators at responsible levels in the organisation?
- For database access, is the OS level file and directory permissions restricted as required for the application?
- Are users denied access to the database other than through the application?
- Are direct query / access to database restricted to the concerned database administrators?
- Whether use of triggers and large queries monitored to prevent overloading of database and consequent degradation of database performance?

Module 3, Chapter 3

- Are all vendor-supplied passwords and default passwords changed? Have all demo user and demo databases removed?
- Are there controls on sessions per user, number of concurrent users, etc?
- Is creation of users is restricted and need based? Are the rights granted to various users reasonable and based on requirement?
- Is the database configured to ensure audit trails, logging of user sessions and session auditing?
- Does the administrator maintain a list of batch jobs executed on each database, severity of access of each batch job and timing of execution?
- Are Batch Error Logs reviewed and corrective action taken by the Administrator periodically?
- Is there a separate area earmarked for temporary queries created by power users or database administrator based on specific user request?
- Are temporary sub databases created removed periodically or after the desired purpose is achieved?
- Does the design or schema of all tables / files in database contain fields for recording makers, checkers and time stamp?
- Are database administrators rotated periodically?
- In cases where data is provided to external service providers does the organisation have confidentiality undertakings from these service providers?

Referential Integrity and Accuracy

- Is there a standard set of database control reports designed in consultation with the user department for ensuring accuracy and integrity of the databases?
- Are these reports run directly from the back-end database periodically and the results both positive and negative are communicated by the administrators to senior management?
- Are these reports run periodically and taken directly by the User Department themselves to ensure accuracy?
- In case of automated interface between systems is there a system of reconciliation between the source and receiving system for critical information?
- In cases where data is migrated from one system to another has the user department verified and satisfied about the accuracy of the information migrated? Is there a formal data migration report?
- Are there entries directly made to the back end databases? If they are made under exceptional circumstances, is there a system of written authorization?

- ▶ If entries in the database are updated / deleted due to any exceptional circumstances (e.g. during trouble shooting, etc.), are they approved in writing and recorded?

Administration and House Keeping

- ▶ Does the administrator periodically review the list of users to the database? Is the review documented?
- ▶ Are inactive users deactivated?
- ▶ Is there a back-up schedule?
- ▶ Are databases periodically retrieved from the back up in test environment and accuracy ensured?
- ▶ Are senior personnel from the user department involved in testing backup retrieval?
- ▶ Is there periodic purging / archival of databases?

Summary

Logical access controls involve securing both resident data and data in transit. In order to secure this data, one of the key steps is authentication. Authentication involves ensuring the genuineness of the identity claimed by the user. Over time various techniques have been developed to provide internal and external access controls. They are systems with varying degrees of reliability, precision, sophistication and cost. Selection of the appropriate logical access methods is a complex decision.

One of the common access control techniques is logon IDs and passwords. In token-based authentication the user possesses identification to enable authentication. Biometrics offers a very high level of authentication based on “what the user is”, based on characteristics of the human body e.g. fingerprints, facial scans, etc.

Compromise of operating systems processing can lead to improper access to system resources. In order to safeguard against improper access, a concept of reference monitor implements logical control over access to object. Reference monitor is an abstract mechanism that enables enforcing the security policy. Relational database security works on the principles of tables and relations and allows rules of integrity and access to be specified. The principle of least privileges to data items can be enforced using views as against reads.

As in any other audit, obtaining an understanding of the environment, evaluation of all related controls and adequate involvement of top management determine the success of the audit. Obtaining an understanding of networking environment plays an important role in such a situation. Understanding networked environment involves obtaining inventory of the various components, security features, security policies etc.

Module 3, Chapter 3

The audit steps involved are identification of logical access paths at all levels like hardware, system software, database management and application control. The various components to be evaluated during such audit are:

- ▶ Testing the appropriateness of system configurations and parameter settings
- ▶ Testing various logical access mechanisms, evaluation of user account management and password management
- ▶ Evaluation of access to file directories and application logic and system instruction set
- ▶ Adequacy of monitoring and reporting procedures and bypass security procedures



4 Application Controls

✂ Learning Goals ✂

To understand:

- ▶ Application Boundary Controls
- ▶ Input Controls
- ▶ Processing Controls
- ▶ Datafile Controls
- ▶ Output Controls

Introduction

Applications represent the interface between the user and the business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his job description and assigned responsibilities. He is able to relate to the advantages of technology when he is able to interact with the computer system from the perspective of meeting his job objectives. From the point of view of users, it is the applications that drive the business logic.

Therefore from an organisational perspective, it is important that the applications:

- ▶ Safeguard assets
- ▶ Maintain data integrity
- ▶ Achieve organisational goals effectively and efficiently

Components of Application Controls

Application controls can be broadly classified as follows:

- ▶ **Boundary Controls:** Controls to ensure that access to the application is restricted only to authorised users and that the application protects systems from unauthorized access.
- ▶ **Input Controls:** Controls to ensure that only complete, accurate and valid data and instructions are input to the application.
- ▶ **Processing Controls:** Controls to ensure that only authorised processing occurs and integrity of processes and data is ensured.
- ▶ **Datafile controls:** Controls to ensure that data resident in the files are maintained consistently with the assurance of integrity and confidentiality of the stored data.
- ▶ **Output Controls:** Controls to ensure that outputs delivered to the users is delivered in a consistent and timely manner in the format and manner prescribed/required by the user.

Each of the above controls are examined in greater detail in the following sections.

Application Boundary Controls

The objective of boundary controls is to prevent unauthorized access to applications and their data. Such data may be in any stage, input, processing, in transit or being output. The controls should restrict user access in accordance with business policy and organisation structure, protect other associated applications, systems software, database and utilities from unauthorized access.

Such access controls may be implemented using any of the logical security techniques being embedded as part of the application software. Besides access security implemented at operating system and/or database management systems level, a separate access control mechanism may be required to be provided for controlling access to application. The application may have boundary controls to ensure adequate access security to prevent any unauthorized access to:

- Applications themselves
- Application data during communication or transit
- Stored application data
- Resources shared with other processes

The above objectives can be achieved by adopting logical security techniques like:

- Using logon ids and passwords.
- Providing access to application from specified terminals only.

Cryptographic Controls

- Encrypting all data leaving and entering the application process.
- Encrypting intermediary data either in input, processing or output stage stored in database.
- Ensuring confidentiality, integrity and availability through encryption and authentication of all exchanges of data/processes between applications. The authentication of users and process usually occur at the network level since it is cumbersome to authenticate for each and every application. See the next chapter for authentication of users at the network layer.

Audit Trail

All significant events that occur at the boundary of the application should be logged. These event include all or any of the following:

- Identity of the user requesting access.
- Authentication supplied by the user.
- Number of incorrect login attempts
- Terminal-id.
- Time of login and log-out.
- Actions permitted/denied.

Input Controls

Input controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important since substantial time is spent on input of data, involve human intervention and are therefore error and fraud prone.

Data Input Methods

Data input pertain either to the state of the object (such as price of a commodity) or event (sale of the commodity). Data input may be done directly into system using devices such as scanners, mouse, touch screens etc. or using an intermediary medium such as a writing on a document (the intermediary medium) and then entering into the system using a keyboard.

Data can be pre-recorded or post-recorded. Pre-recorded means that it is recorded prior to the occurrence of event or detection of state of the object. For example, the price of goods may be recorded on an item by affixing a magnetic strip that contains the price before the item is sold. In the case of post recording, the event is recorded only after it occurs, such as, a sale transaction in which the quantity of products purchased is entered only after the customer purchases the product.

Source Document Design

Source documents are used as an intermediary medium to record data before being input into the system, such as a sales invoice prepared manually using a typewriter in a branch office for want of computer infrastructure. A well-designed source document helps improve control in the following ways:

- ▶ It reduces data entry errors
- ▶ Increases speed of data entry
- ▶ Ensures better control over the process
- ▶ Assists subsequent reference

Source document design begins with an analysis of the need and usage of the source document. Source document design includes the following:

- ▶ Material to be used for the source document.
- ▶ Layout and style of the source document.

In designing the layout of the source document the following should be kept in mind:

- ▶ Include instructions for completing the form.
- ▶ Minimize the amount of handwriting.
- ▶ Data to be entered (keyed) should be sequenced so that it can be read like a book, that is, top-to-bottom and left-to-right.
- ▶ Capture only variable data.

Module 3, Chapter 4

- ▶ Do not capture data that can be calculated or stored in computer programs as constants.
- ▶ Use organization wide consistent business codes for appropriate attributes.

Data entry screen design

Data is keyed into online forms or tables. The system plays a role in the data entry process, guiding users who need help, checking data entries to detect errors, and providing other kinds of data processing aids. A designer of user interface software must be concerned about computer processing logic as well as data input by the user. While data entry is heavily emphasized in clerical jobs, all jobs involve data entry to some degree, in the modern enterprise. The general objectives of designing good data entry screens are to establish consistency of data entry transactions, minimize input actions and resource requirements on the system, ensure compatibility of data entry with data display, and provide flexibility of user control of data entry. Auditors must be able to evaluate the data entry screens and come to a judgement about the possible extent of errors that may propagate. This judgement will affect the extent of their checking.

The factors that should be considered while designing data entry screens are detailed below.

Screen organisation

Good screen designs are symmetric. Further, screens should be uncluttered and easily to follow the pattern of data flow. With increase in data elements, the complexity increases and therefore multiple screens with a logical changeover should be used. As much as possible where a source document is involved, the screen organization should be identical to the source document. Consistency of the screen layout should be ensured and the same design should be repeated wherever possible.

Caption design

Captions guide the users as to the nature of the data to be entered. Some of the points that are to be considered are as follows:

- ▶ Make field captions consistent; always employ the same caption to indicate the same kind of data entry.
- ▶ Ensure that captions are sufficiently close to be associated with their proper data fields, but are separated from data fields by at least one space.
- ▶ Make captions for data fields distinctive, so that they will not be readily confused with data entries, labelled control options, guidance messages, or other displayed material.
- ▶ The caption for each entry field should end with a special symbol(":"), signifying the start of the entry area.

- ▶ Captions should employ descriptive wording, or else standard, pre-defined terms, codes and/or abbreviations; avoid arbitrary codes.

Data entry field design

Data entry fields should be either to the right of the caption or exactly below it. Provide underscores in fields to indicate when a fixed or maximum length is specified for a data entry. Where source documents are used the pattern should be based on the source document. Option buttons and check boxes should be used when the user has to choose from a small list of options. In case user has to choose from a long list of options, list boxes can be used.

Tabbing and skipping

During data entry, the user moves from field to field by pressing the “Tab” key. It is important to ensure the Tab order is consistent, so that the insertion point moves from the first field on the screen to the last without jumping about. Incorrect tab order will not only frustrate users, but it may cause them to enter data into the wrong field. Automatic tabbing should be avoided since fields may be skipped for data entry.

Colour

Colours help reduce search time and make the screen more interesting. However, bad usage of colour may distract or confuse the users. The following should be kept in mind when deciding the colours.

- ▶ Bright colours should be avoided. Instead choose soft or pastel colours or those that provide good contrast for the fields and captions.
- ▶ Uppercase and lowercase may be used to differentiate captions, if the display is monochrome or if the users have difficulty in distinguishing colours due to eye defects, poor or excessive lighting, etc.

Response time

Response time is the interval between entry of data item and the system’s indication that it has been stored and is ready for new data. Response time should be as low as possible and should be reasonably constant throughout.

Display rate

Display rate is the rate at which characters or images should be displayed. Data entry screens should have a fast and consistent display rate. If display rate is slow or inconsistent the data entry is prone to errors.

Prompting and help facilities

Descriptive help should be added wherever possible. Data entry forms should be as self-explanatory as possible but can include help for each field. Prompting of actions that should be taken by the user can be provided by using pop-up messages that appear on placing the cursor on

Module 3, Chapter 4

a field. More prompting and help is required in the case of direct data entry where no source document is involved.

Data code controls

Data codes are used to uniquely identify an entity or identify an entity as a member of a group or set. Auditors should evaluate the quality of coding systems to analyse their impact on the integrity and accurateness of data keyed into the system.

Types of data coding errors:

- ▶ **Addition:** Addition of an extra character in a code
- ▶ **Truncation:** Omission of characters in the code
- ▶ **Transcription:** Recording wrong characters
- ▶ **Transposition:** Reversing adjacent characters
- ▶ **Double transposition:** Reversing characters separated by one or more characters i.e., 45123 is entered as 42153

Factors affecting coding errors as follows:

- ▶ **Length of the code:** Long codes are naturally prone to more errors. Long codes should be broken using hyphens, slashes or spaces to reduce coding errors.
- ▶ **Alphabetic numeric mix:** The code should provide for grouping of alphabets and numerical separately if both are used. Intermingling both would result in more errors.
- ▶ **Choice of characters:** Certain alphabets are confused with numerical such as B, I, O, S, V and Z would be confused with 8,1,0,5,U, 2 when written on source document and entered into the system. Such as characters should be avoided
- ▶ **Mixing uppercase/lowercase fonts:** Upper case and lower case should NOT be mixed when using codes since they delay the process of keying in due to usage of the shift key. Further such codes are prone to errors.
- ▶ **Sequence of characters:** Character sequence should be maintained as much as possible. Such as using ABC instead of ACB.

Check digits

Check digits are redundant digits that helps verify the accuracy of other characters in the code that is checked. The program recalculates the check digits and compares with the check digit in the code when the code is entered to verify if the code is correct. Check digits may be prefixes or suffixes to the actual data. Since check digits are redundant data and take time to calculate they should be used only on critical fields.

Batch Controls

Batch controls group input transactions into logical or physical batches. Physical batches are groups of transactions that constitute a physical

unit such as a set of invoices pertaining to a branch bundled up together. Logical batches are groups of transactions that are divided on a logical parameter such as cut off date, documents pertaining to division or branch.

Control over physical batches are ensured through batch header forms, which are data preparation sheets containing control information about the batch.

Types of batch controls are as follows:

- ▶ **Total financial amount:** Counter-checking that the total financial amount of items processed in that batch with the total individual financial amounts in the fields. For example, if a batch of 100 invoices are processed, it should be verified that the gross total of individual item sale value in the invoices match the total value of sales of all the invoices processed.
- ▶ **Total items:** Counter-checking that the total number of items included on each document in the batch matches the total number of items processed. For example, the total number of units sold as per each invoice should match the total number of items processed in the batch.
- ▶ **Hash totals:** Hash totals are totals of any numeric field in the batch such as serial number of invoices to counter check the total of the field after input of data.
- ▶ **Total documents:** Total number of documents processed should also be counterchecked for correctness.

Data Input Validation

Input Authentication Controls

One of the important objectives of application controls is to ensure that the data that is input into the application is valid or authorised. This can be ensured in many ways, some of which are given below:

- ▶ Manual signatures on input document
- ▶ In case of online inputs, Input menu available for specified logins only to ensure that personnel having authority only enter the document and are accountable for the transaction they enter. Further input may be restricted only through predetermined specified terminals.
- ▶ Restricting certain types of input to be enabled only on unique passwords at the input menu level.
- ▶ Scanned Input using OCR (Optical Character Recognition), Barcode Readers, MICR (Magnetic Ink Character Recognition), etc.

The input system should validate the data that is submitted for processing as close to the point of origin as possible. Data validation controls identify data errors, incomplete or missing data and inconsistencies among related data items. Normally data validation controls are preven-

Module 3, Chapter 4

tive in nature since they ensure incorrect data is not entered in the system. Edit controls are the principal data validation controls and are used to validate data.

Edit Controls

Sequence checks: Controls that verify if the data maintains a proper sequence or order. Usually used to check serial numbers of documents, or the date sequence of transactions.

Range and Limit check: Range check refers to fixing an upper and lower limit for data values to ensure they don't exceed them. Limit checks refer to only upper or lower limit of data values, but not both. For example, if the edit check requires that gross salary should not exceed Rs.100,000/- per month, it is a limit check. If the check requires that percentage of tax should minimum of 10% and maximum of 30% on the gross total income, it is a range check.

Missing data check: Ensures that certain key fields are not left blank during data entry.

Duplicate check: Duplicate check ensures that the same data is not keyed twice. For example when entering invoices the same invoice number should not be repeated twice.

Programmed Validity Check: Logical validations may be set within the application code to check for invalid input for example a user may be prevented from entering a non existent account code.

Dependency Match: Where certain fields depend on input values in other fields, programmed checks can be used for internally validated data before accepting input e.g. Date of joining may be compared to the date of birth to ensure that the latter is earlier than the former.

Completeness check: Completeness of data may be checked before accepting data entered. For example, while creating a new e-mail user id, the input screen will not be accepted without date of birth, name, address etc. (marked as required fields).

Reasonableness check: Reasonable of value entered may be compared with an acceptable range within the system before accepting input, e.g. age entered as 140 may be rejected as unreasonable.

Table lookups: Input entered is matched with a range of values in table before acceptance. E.g. customer code entered by the operator is internally matched with a table of valid customers for a successful match, else transaction is rejected.

Data Input Error Handling and Reporting

Input error handling and reporting requires that controls that identify errors and correct them especially in a batch processing system where input and validation may take place at different points of time. Input errors can be handled in the following ways:

Rejecting only transaction with errors: Only those transactions containing the errors would be rejected and the rest of the batch would be processed.

Rejecting the whole batch of transactions: The whole batch of transactions is rejected if even one error is found in the batch. This is usually done in cases where transactions have to be in a sequential order and data entry has not been made in a sequential order.

Accepting batch in suspense: The batch would be held in suspense till the corrections in transactions are made. However the batch or the transactions are not rejected.

Accepting the batch and marking error transactions: Erroneous transactions are separately marked for identifying later and the whole batch is processed. This is usually done in an online system.

Instruction Input Controls

Validating instructions is more difficult than validating data. This is due to fact that instruction input requires more user interaction and decision discretion than in the case of data input. However, auditors should ensure that users are brought under a set of action privileges and their instructions are controlled and logged.

Instruction input methods

There are different types of interfaces to give instructions depending upon the application system and extent of control to be exercised on them. Some of the instructions interfaces that are available are as follows:

Menu Driven Applications: These applications provide a set of instructions that are fixed and the users only need to choose the actions to be done depending on the options available in the menu. Such instructions can be well controlled since the choices available to users can be restricted based on the content and context.

Question Answer dialogs: These are mainly used for capturing user preferences and occasionally data. These interfaces ask a series of questions to the user and provide a set of options from which the user is required to make a selection. For example, a financial software may ask the user a series of questions regarding present value, interest rate, periodicity of payment, etc. and then provide the requisite output.

Command Languages: These are languages, which requires users to specify commands to the system complete a set of processes. Each command may have several parameters, that modify the behaviour of the command. The DOS operating system is an example of a command based operating system. Structured query language (SQL) which is used to interrogate databases is another example of command language.

Direct Manipulation interfaces: Many personal productivity software like electronic spreadsheets, word processors, employ direct manipulation interface to carry out commonly used functions, and input data. Direct manipulation interfaces offer lot of flexibility and speed and are relatively error free.

Instruction Input Validation

Instructions are subject to three validation checks, (1) Lexical, (2) Syntactic and (3) Semantic checks.

Lexical validation

Each word entered as a instruction is validated to ensure its correctness.

Syntactic validation

System reads a string of words validated by the lexical analyzer and attempts to ensure that the sequence of operations is correct.

Semantic validation

Semantic validation reads the set of instructions and verifies if the meaning is correct. For example if a command in SQL is as follows:
Select NAME from EMPLOYEE where EMPCODE = 10001

The semantic analyzer would ensure that there exists a table “EMPLOYEE” in which fields of names “NAME” and “EMPCODE” and exists.

Reporting Instruction Input Errors

Error messages of instructions must be communicated to users as early as possible. The error messages must complete and meaningful and help the user correct it immediately. Different error messages may be given based on the expertise of user.

Processing Controls

Data processing controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. Normally the processing controls are enforced through the database management system that stores the data. However, adequate controls should be enforced

through the front end application system also to have consistency in the control process.

Data processing controls

Run-to-run totals: These help in verifying data that is subject to process through different stages. If the current balance of an invoice ledger is Rs.150,000 and the additional invoices for the period is of total Rs.20,000 then the total sales value should be Rs.170,000. A specific record (probably the last record) can be used to maintain the control total.

Reasonableness verification: Two or more fields can be compared and cross verified to ensure their correctness. For example the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.

Edit checks: Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.

Field initialization: Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e., setting all values to zero before inserting the field or record.

Exception reports: Exception reports are generated to identify errors in data processed. Such exception reports give the transaction code and why the particular transaction was not processed or what is the error in processing the transaction. For example, while processing a journal entry if only debit entry was updated and the credit entry was not updated due to absence of one of the important fields, then the exception report would detail the transaction code, and why it was not updated in the database.

Datafile Controls

Version usage: Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.

Internal and external labelling: Labelling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process of loading files external labelling is important to ensure that the correct file is being processed. Where there is a automated tape loader system, internal labelling is more important.

Data file security: Unauthorized access to data file should be prevented, to ensure confidentiality, integrity and availability of the data file for process. These controls are aimed at ensuring that the correct file is used for processing and do not consider the data's validity

Before and after image and logging: The application may provide for reporting of before and after images of transactions. Before and after images combined with logging of events enable re-constructing the datafile back to its last state of integrity, after which the application can ensure that the incremental transactions/events can be rolled back or forward.

File updating and maintenance authorization: Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or as part of the overall system access restrictions.

Parity Checking: When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error detecting or correcting codes.

Output Controls

Output controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form, it can either be a printed data report or a database file in a removable media such as a floppy disk or CD-ROM or it can be a Word document on the computer's hard disk. Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained and that the output is consistent. Output controls have to be enforced both in a batch-processing environment as well as in an online environment.

Output controls

Storage and logging of sensitive, critical forms: Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments etc.

Logging of output program executions: When programs used for output of data are executed, it should be logged and monitored. In the absence of control over such output program executions, confidentiality of data could be compromised.

Spooling/Queuing: "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user is able to continue working, even before the print operation is completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is then "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer. This queue should not be subject to unauthorized modifications.

Controls over printing: Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed is prevented. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.

Report distribution and collection controls: Distribution of reports should be made in a secure way to ensure unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained as to what reports were generated and to whom it was distributed. Where users have to collect reports the user should be responsible for timely collection of the report especially if it is printed in a public area. A log should be maintained as to what reports were printed and which of them were collected. Uncollected reports should be stored securely.

Retention controls: Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.

Online output controls

Factors that are affecting online output issues and controls are a) increase in amount of online output and controls need for online output b) variety of online output ranging from text and graphics to images and media files. c) growth of Internet and possibility of using unsecured channels of communication.

Source controls: Source controls ensure that the source of the output is accurate, complete and consistent. For example if a user accesses a database for obtaining information, the source database should be accurate and complete. In addition to this the program used to access the source information should also be authorized to access the information in the database.

Distribution controls: Similar to distribution of reports and output in a batch control environment, proper controls should exist to ensure that only the right persons receive the output. If email systems are used, the recipients' email address should be verified periodically.

Communication controls: Communication of output should be well defined and follow a clear process that has an appropriate audit trail.

Module 3, Chapter 4

Cryptographic systems may be used to ensure confidentiality and integrity of communication in electronic data interchange systems (EDI).

Receipt controls: Receipt controls verify if the output should be accepted for further process and whether output that was to be received has actually been received.

Retention and deletion controls: Unnecessary wastage of resources may take place with retention of output beyond the required time period. The system should have a retention period for the output after which the output should be purged or deleted. Statutory requirements should also be considered before deciding file retention period. Deletion controls should ensure deletion of the appropriate output as required by the user and based on the retention period. In addition to this, it should be ensured that deleted records are not stored in temporary file locations giving rise to unauthorized access.

Existence Controls in Application Systems

Existence controls are those controls that ensure the continued availability of the application system and data in a consistent manner to the users. Existence controls form an integral part of the input, processing and output controls. Recovery of the application system from failures and restoration of both standing data as well as transaction data is very critical. Therefore, existence controls should include backup and recovery procedures of data. This requires secure storage of data files. Existence controls over processing of data should include adequate checkpoint/restart controls that recover process from a failure without having to repeat the entire process from the beginning. Existence controls should also be exercised over output to prevent loss of output of any form i.e., paper, spool files, output files etc. Finally recovering the application system accurately, completely and promptly can be critical to many organizations especially if they are in an EDI environment.

Audit of Application Controls

The audit of application controls requires the IS auditor to ensure that the application system under audit:

- ▶ Safeguards organisational assets
- ▶ Maintains data integrity
- ▶ Achieves organisational goals effectively
- ▶ Consumes resources efficiently

Review of application controls

When reviewing the application controls, the IS auditor should ensure that the audit objectives with regard to confidentiality, integrity and availability of organisational information are orderly and complete.

The process of application control review:

1. Obtaining preliminary information

1. Based on general understanding of the business process and risks assessment, the IS auditor should determine the application owners and users.
2. Determine the application objectives, functionality and features that map onto the business process(es) of the organisation to determine if functional design incorporates key control points.
3. In case of applications developed in-house determine if the controls systems development methodology were adequate and in the case of bought-out applications determine if there are adequate controls in respect of escrows, warranties and support.
4. Determine the IT environment in which the application is installed and operates. This would include gaining an understanding of the hardware, networking, operating systems and other systems software. The technical and administration manual, programmer manual and user manual must contain information relevant to this context.

2. Determine whether:

1. The application provides adequate level of access controls protecting the application data and application program. The access controls should also guard against covert channels and provide for inference controls. Besides providing adequate preventive access controls, the auditor should determine if the application provides for detective control such as check sums, audit trails, and transaction logs. Where the application interfaces with an access control software or other such mechanism, there should be seamless security.
2. Controls over the preparation, collection, and processing of source documents ensure the accuracy, completeness and timeliness of data before they reach the application.
3. Manual and automated controls over data entry (batch or online), data validation, error identification and reporting are adequate and effective. Also ensure that error correction and re-entry is effective and the data is completely and accurately entered into the application.
4. Controls over application programs and related computer operations to ensure the accuracy, completeness, and timeliness of data during batch or real time processing are adequate and effective.
5. Controls over file handling, file access, and backup and recovery are effective and adequate. This is necessary to ensure the completeness and accuracy of data during the process of data storage and retrieval.
6. Controls over balancing and reconciliation, distribution of output, handling of negotiable documents, and output retention are effective.

Module 3, Chapter 4

tive to ensure that output is accurate and distributed to authorised personnel on a timely basis.

Summary

Applications are directly related to users and their requirement and business functions. Application controls safeguard assets, maintain the integrity of data and achieve organisational goals, effectively and efficiently. Application controls can be broadly categorized as boundary controls, input controls, processing controls, data file controls, output controls and existence controls. Boundary controls prevent unauthorized access to applications and application data. Input controls ensure the accuracy and completeness of data and instructions input into an application system. The input entering the application should be received completely, it should be accurate and valid. Data processing controls perform validation checks to identify errors while processing data. They are required to ensure both the completeness and the accuracy of the data being processed. Output controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Existence controls are controls that ensure the continued availability of the application system and data in a consistent manner to the users. They form an integral part of the input, processing and output controls.



5 Network Security Controls

✂ Learning Goals ✂

To understand:

- ▶ Characteristics of a network
- ▶ The threats facing a network
- ▶ The controls that can protect a network

Introduction

In this section, we examine the risks and controls that are specific to networked computers. It is rare these days to find a standalone computer in any commercial environment, as networks offer tremendous advantages that far outweigh the cost of creating them. However, networks are also far more vulnerable to external and internal threats than are standalone systems. The biggest network of all is the Internet, the network of networks. However, the Internet while offering tremendous advantages also poses several security challenges to organisations. In this section, we shall look at threats and risks that arise in a networked environment and the controls and countermeasures that prevent or mitigate such risks.

Network Characteristics

A network in its simplest form, is two devices connected across some medium by hardware and software that enable communication between the two. In some cases, one device is a computer (sometimes called a “server”) and the other is a simpler device (sometimes called a “client”) enabled only with some means of input (such as a keyboard) and some means of output (such as a screen). For example, a powerful computer can be a server, but a handheld personal digital assistant (PDA) or a cell phone might be a network client.

Although this model defines a basic network, in practice, the situation is significantly more complicated:

- ▶ The simpler client device, employed for user-to-computer communication, is often a PC or workstation, so the client has considerable storage and processing capability.
- ▶ A network can be configured as just a single client connected to a single server. But more typically, many clients interact with many servers.
- ▶ The network’s services are often provided by many computers. As a single user’s communication travels back and forth from client to

Module 3, Chapter 5

server, it may merely pass through some computers but pause at others for significant interactions.

- ▶ The end user is usually unaware of many of the communications and computations taking place in the network on the user's behalf.

Networks can be described by several common characteristics:

- ▶ **Anonymity:** A network removes most of the clues, such as appearance, voice, or context, by which we recognize acquaintances.
- ▶ **Automation:** In some networks, one or both endpoints, as well as all intermediate points, involved in a given communication may be machines with only minimal human supervision.
- ▶ **Distance:** Many networks connect endpoints that are physically far apart. Although not all network connections involve distance, the speed of communication is fast enough that humans usually cannot tell whether a remote site is near or far.
- ▶ **Opacity:** Because the dimension of distance is hidden, users cannot tell whether a remote host is in the room next door or in a different country. In the same way, users cannot distinguish whether they are connected to a node in an office, school, home, or warehouse, or whether the node's computing system is large or small, modest or powerful. In fact, users cannot tell if the current communication involves the same machine with which they communicated the last time.
- ▶ **Routing diversity:** To maintain or improve reliability and performance, routings between two endpoints are usually dynamic. That is, the same interaction may follow one path through the network the first time and a very different path the second time. In fact, a query may take a different path from the response that follows a few seconds later.

Threats and Vulnerabilities

This section describes the various kinds of vulnerabilities and threats that aim to compromise the confidentiality, integrity, or availability of data, software and hardware by accidents, non-malicious humans, and malicious attackers. The threats and vulnerabilities are listed under the following heads:

- ▶ Information Gathering
- ▶ Communication Subsystem Vulnerabilities
- ▶ Protocol Flaws
- ▶ Impersonation
- ▶ Spoofing
- ▶ Message Confidentiality Threats
- ▶ Message Integrity Threats
- ▶ Web Site Defacement
- ▶ Denial of Service

- Distributed Denial of Service
- Threats from Cookies, Scripts and Active or Mobile Code

Information Gathering

An attacker does not just sit at a computer and launch an attack without prior planning. Instead, a serious attacker will spend a lot of time obtaining as much information as s/he can about the target before launching an attack. The tools and techniques to gather information about the attack are examined below:

- **Port Scan:** An easy way to gather network information is to use a port scanner, a program that, for a particular IP address, reports which ports respond to messages and which of several known vulnerabilities seem to be present.
- **Social Engineering:** Social engineering involves using social skills and personal interaction to get someone to reveal security-relevant information and perhaps even to do something that permits an attack. The point of social engineering is to persuade the victim to be helpful. The attacker often impersonates someone occupying a senior position inside the organization who is in some difficulty. The victim provides the necessary assistance without verifying the identity of the caller, thus compromising security.
- **Reconnaissance:** Reconnaissance is the general term for collecting information. In security, it often refers to gathering discrete bits of information from various sources and then putting them together to make a coherent picture. One commonly used reconnaissance technique is “dumpster diving.” It involves looking through items that have been discarded in garbage bins or waste paper baskets. One might find network diagrams, printouts of security device configurations, system designs and source code, telephone and employee lists, and more. Even outdated printouts may be useful. Reconnaissance may also involve eavesdropping. The attacker or his accomplice may follow employees to lunch and listen in from nearby tables as co-workers discuss security matters.
- **Operating System and Application Fingerprinting:** Here the attacker wants to know which commercial server application is running, what version, and what the underlying operating system and version are. While the network protocols are standard and vendor independent, each vendor has implemented the standard independently, so there may be minor variations in interpretation and behaviour. The variations do not make the software noncompliant with the standard, but they are different enough to make each version distinctive. How a system responds to a prompt (for instance, by acknowledging it, requesting retransmission, or ignoring it) can also reveal the system and version. New features also offer a clue, for example a new version will implement a new feature but an old version will reject the re-

Module 3, Chapter 5

quest. All these peculiarities, sometimes called the operating system or application fingerprint, can mark the manufacturer and version.

- ▶ **Bulletin Boards and Chats:** Underground bulletin boards and chat rooms support exchange of information among the hackers. Attackers can post their latest exploits and techniques, read what others have done, and search for additional information on systems, applications, or sites.
- ▶ **Documentation:** The vendors themselves sometimes distribute information that is useful to an attacker. For example, resource kits distributed by application vendors to other developers can also give attackers tools to use in investigating a product that can subsequently be the target of an attack.

Communication Subsystem Vulnerabilities

- ▶ **Eavesdropping and Wiretapping:** An attacker can pick off the content of a communication passing in unencrypted form. The term eavesdrop implies overhearing without expending any extra effort. For example, an attacker (or a system administrator) is eavesdropping by monitoring all traffic passing through a node. (The administrator might have a legitimate purpose, such as watching for inappropriate use of resources.) A more hostile term is wiretap, which means intercepting communications through some effort. Passive wiretapping is just “listening,” just like eavesdropping. But active wiretapping means injecting something into the communication stream. A wiretap can be done in such a manner that neither the sender nor the receiver of a communication will know that the contents have been intercepted. However, signals on a network are multiplexed, which means that more than one signal is transmitted at a given time. This makes the job of extracting the desired data stream more difficult.
- ▶ **Microwave:** Microwave signals are broadcast through the air, making them more accessible to outsiders. An attacker can intercept a microwave transmission by interfering with the line of sight between sender and receiver. It is also possible to pick up the signal from an antenna located close to the legitimate antenna.
- ▶ **Satellite Communication:** In satellite communication, the potential for interception is even greater than with microwave signals. However, because satellite communications are heavily multiplexed, the cost of extracting a single communication is rather high.
- ▶ **Optical Fiber:** It is not possible to tap an optical system without detection. Further optical fiber carries light energy, not electricity, which does not emanate a magnetic field as electricity does. Therefore, an inductive tap is impossible on an optical fiber cable. However, the repeaters, splices, and taps along a cable are places at which data may be intercepted more easily than in the fiber cable itself.

- ▶ **Wireless:** Wireless networking is becoming very popular, but threats arise in the ability of intruders to intercept and spoof a connection. A wireless signal is strong for approximately 30 to 60 metres. A strong signal can be picked up easily. And with an inexpensive, tuned antenna, a wireless signal can be picked up from almost a kilometre away. Interception of wireless traffic is always a threat, through either passive or active wiretapping. The threat can be controlled by encryption, however, encryption is not always used for wireless communication, and the encryption built into some wireless devices is not as strong as it should be to deter a dedicated attacker. Wireless also has a second problem, the possibility of unauthorized use of a network connection, or a theft of service.

Protocol Flaws

Internet protocols are publicly posted for scrutiny. Many problems with protocols have been identified by reviewers and corrected before the protocol was established as a standard. Despite this process of peer review, flaws exist in many of the commonly used protocols. These flaws can be exploited by an attacker.

Impersonation

In many instances, an easy way to obtain information about a network is to impersonate another person or process. Impersonation is a more significant threat in a wide area network than in a local one.

An impersonator may foil authentication by any of the following means:

- ▶ **Authentication foiled by guessing:** Guess the identity and authentication details of the target, by using common passwords, the words in a dictionary, variations of the user name, default passwords, etc.
- ▶ **Authentication foiled by eavesdropping or wiretapping:** In distributed environments, the account and authentication details of the subject are passed to the destination host. When these details are passed on the network, they are exposed to anyone observing the communication on the network. These same authentication details can be reused by an impersonator until they are changed. Because transmitting a password in the clear is a significant vulnerability, protocols have been developed so that the password itself never leaves a user's workstation. Instead the password is transmitted in encrypted form. Despite this encryption, vulnerabilities may remain because implementation deficiencies.
- ▶ **Authentication Foiled by Avoidance:** As an example, a flaw in a particular operating system meant that the buffer for typed characters in a password was of fixed size, counting all characters typed, including backspaces for correction. If a user typed more characters than the buffer would hold, the overflow caused the operating system to by-

Module 3, Chapter 5

pass password comparison and act as if a correct authentication had been supplied. Such flaws or weaknesses can be exploited by anyone seeking unauthorized access.

- ▶ **Nonexistent Authentication:** Here the attacker circumvents or disables the authentication mechanism at the target computer. For example, if two computers are used by the same users to store data and run processes and if each has authenticated its users on first access, it might be assumed that computer-to-computer or local user-to-remote process authentication is unnecessary. However this assumption is not valid. An attacker may obtain access to one system through an authentication weakness (such as a guessed password) and then transfer to another system that accepts the authenticity of a user who comes from a system on its trusted list. An attacker may also use a system that has some identities requiring no authentication. For example, some systems have “guest” or “anonymous” accounts to allow outsiders to access things the systems want to release to the public. These accounts allows access to unauthenticated users.
- ▶ **Well-Known Authentication:** Authentication data should be unique and difficult to guess. However, vendors often sell computers with one system administration account installed, having a default password. Or the systems come with a demonstration or test account, with no required password. Some administrators fail to change the passwords or delete these accounts, creating a vulnerability.

Spoofing

Impersonation falsely represents a valid entity in a communication. Closely related is spoofing, when an attacker falsely carries on one end of a networked interchange. Examples of spoofing are masquerading, session hijacking, and man-in-the-middle attacks.

- ▶ **Masquerade:** In a masquerade one host pretends to be another. A common example is URL confusion. Domain names can easily be confused, or someone can easily mistype certain names. Names with or without hyphens (coca-cola.com versus cocacola.com) and easily mistyped names (citibank.com versus citybank.com) are candidates for masquerading. For example, the attacker wishes to target, say Citibank, he registers the domain citybank.com and makes it look as closely as possible to real Citibank site. Unwary customer are asked to log in with their name, account number, and password or PIN. After collecting the personal data, the attacker can transfer this connection smoothly to an authenticated access to the real Citibank so that the user never realizes the deception.
- ▶ **Session Hijacking:** Session hijacking is intercepting and carrying on a session begun by another entity. Suppose two entities have entered into a session but then a third entity intercepts the traffic and carries

on the session in the name of the other. For example, in an e-commerce transaction, just before a user places his order and gives his address, credit number etc. the session could be hijacked by an attacker.

- ▶ **Man-in-the-Middle Attack:** A man-in-the-middle attack is similar to session hijacking, in which one entity intrudes between two others. The difference between man-in-the-middle and hijacking is that a man-in-the-middle usually participates from the start of the session, whereas a session hijacking occurs after a session has been established. The difference is largely semantic and not particularly significant.

Message Confidentiality Threats

An attacker can easily violate message confidentiality (and perhaps integrity) because of the public nature of networks. Eavesdropping and impersonation attacks can lead to a confidentiality or integrity failure. Here we consider several other vulnerabilities that can affect confidentiality.

- ▶ **Misdelivery:** Sometimes messages are mis-delivered because of some flaw in the network hardware or software. Most frequently, messages are lost entirely, which is an integrity or availability issue. Occasionally, however, a destination address will be modified or some router or protocol will malfunction, causing a message to be delivered to someone other than the intended recipient. All of these “random” events are quite uncommon. More frequent than network flaws are human errors, caused by mistyping an address.
- ▶ **Exposure:** The content of a message may be exposed in temporary buffers, at switches, routers, gateways, and intermediate hosts throughout the network; and in the workspaces of processes that build, format, and present the message. A malicious attacker can use any of these exposures as part of a general or focused attack on message confidentiality. Passive wiretapping is one source of message exposure. So also is subversion of the structure by which a communication is routed to its destination. Finally, intercepting the message at its source, destination, or at any intermediate node can lead to its exposure.
- ▶ **Traffic Analysis (or Traffic Flow Analysis):** Sometimes not only is the message itself sensitive but the fact that a message exists is also sensitive. For example, if a wartime enemy sees a large amount of network traffic between headquarters and a particular unit, the enemy may be able to infer that significant action is being planned involving that unit. In a commercial setting, messages sent from the president of one company to the president of a competitor could lead to speculation about a takeover or conspiracy to fix prices. In these cases, we

Module 3, Chapter 5

need to protect both the content of messages and the header information that identifies sender and receiver.

Message Integrity Threats

In most cases, the integrity or correctness of a communication is more important than its confidentiality. Some of the threats which could compromise integrity are by:

- ▶ Changing some or all of the content of a message
- ▶ Replacing a message entirely, including the date, time, and sender/receiver identification
- ▶ Reusing (replaying) an old message
- ▶ Combining pieces of different messages into one false message
- ▶ Changing the apparent source of a message
- ▶ Redirecting a message
- ▶ Destroying or deleting a message

These attacks can be perpetrated in the ways already stated, including:

- ▶ Active wiretap
- ▶ Trojan horse
- ▶ Impersonation
- ▶ Compromised host or workstation

Web Site Defacement

Web site defacement is common not only because of its visibility but also because of the ease with which one can be done. Web sites are designed so that their code is downloaded to the client (browser), enabling an attacker to obtain the full hypertext document and all programs and references programs embedded in the browser. This essentially gives the attacker the information necessary to attack the web site. Websites have many common and well known vulnerabilities that an attacker can exploit.

Denial of Service

Denial of Service (DoS) attacks lead to loss of network availability. The physical threats are obvious, such as someone maliciously cutting a cable. The electronic threats are more serious and less obvious. Some of the are described below:

- ▶ **Connection Flooding:** This is the oldest type of attack where an attacker sends more data than what a communications system can handle, the systems is prevented from receiving any other legitimate data. Even if an occasional legitimate packet reaches the system, communication will be seriously degraded.
- ▶ **Ping of death:** More sophisticated attacks exploit features of internet protocols, like TCP, UDP and ICMP (Internet Control Message Protocols). Such attacks are difficult to detect in advance or block at the receiving end. Ping is an ICMP protocol which requests a desti-

nation to return a reply, intended to show that the destination system is reachable and functioning. Since ping requires the recipient to respond to the ping request, all the attacker needs to do is send a flood of pings to the intended victim.

- ▶ **Traffic Redirection:** A router is a device that forwards traffic on its way through intermediate networks between a source host's network and a destination's. So if an attacker can corrupt the routing, traffic can disappear.
- ▶ **DNS Attacks:** DNS attacks are actually a class of attacks based on the concept of domain name server. A domain name server (DNS) is a table that converts domain names like `www.icai.org` into network addresses like `202.54.74.130`, a process called resolving the domain name. By corrupting a name server or causing it to cache spurious entries, an attacker can redirect the routing of any traffic, or ensure that packets intended for a particular host never reach their destination.

Distributed Denial of Service

An attacker can construct a two-stage DoS attack that multiplies the destructive effect many times. To perpetrate a distributed denial-of-service (or DDoS) attack, an attacker does two things. In the first stage, the attacker uses any convenient attack (such as exploiting a buffer overflow or tricking the victim to open and install unknown code from an e-mail attachment) to plant a Trojan horse on a target machine. This Trojan horse does not necessarily cause any harm to the target machine so can remain undetected. The attacker repeats this process with many such targets. Each of these target systems is called **ZOMBIE**. At some point the attacker chooses a victim and sends a signal to all the zombies to launch the attack. Then, instead of the victim's trying to defend against one denial-of-service attack from one malicious host, the victim must try to counter attacks from the all zombies acting at once. In addition to their tremendous multiplying effect, distributed denial-of-service attacks are a serious problem because they are easily launched from scripts.

Threats from Cookies, Scripts and Active or Mobile Code

Some of the vulnerabilities relating to data or programs that are downloaded from the server and used by the client are as follows:

- ▶ **Cookies:** Cookies are NOT executable. They are data files created by the server, that can be stored on the client machine and fetched by a remote server usually containing information about the user on the client machine. Anyone intercepting or retrieving a cookie can impersonate the cookie's legitimate owner.
- ▶ **Scripts:** Clients can invoke services by executing scripts on servers. A malicious user can monitor the communication between a browser

and a server to see how changing a web page entry affects what the browser sends and then how the server reacts. With this knowledge, the malicious user can manipulate the server's actions. The common scripting languages for web servers, CGI (Common Gateway Interface), and Microsoft's active server pages (ASP) have vulnerabilities that can be exploited by an attacker.

- ▶ **Active Code:** Active code or mobile code is a general name for code that is downloaded from the server by the client and executed on the client machine. The popular types of active code languages are Java, JavaScript, VBScript and ActiveX controls. Such executable code are also called applets. A hostile applet is downloadable code that can cause harm on the client's system. Because an applet is not screened for safety when it is downloaded and because it typically runs with the privileges of its invoking user, a hostile applet can cause serious damage.

Network Security Controls

This section examines the controls available to ensure network security from the various threat identified listed earlier. The controls are listed under the following broad heads

- ▶ Architecture
- ▶ Cryptography/Encryption
- ▶ Content Integrity
- ▶ Strong Authentication
- ▶ Remote Access Security
- ▶ Firewalls
- ▶ Intrusion Detection Systems

Architecture

The architecture or design of a network can have a significant effect on its security. Some of the major considerations are:

- ▶ **Segmentation:** Segmentation can limit the potential for harm in a network in two important ways. Segmentation reduces the number of threats, and it limits the amount of damage a single vulnerability can allow. For example, if a web server, authentication software, applications and database are residing on a single server for facilitating electronic commerce transactions, then it results in a very insecure configuration. A more secure design uses multiple segments. Since the web server has to be exposed to the public, that server should not have other, more sensitive, functions on it, such as user authentication or access to the database. Separate segments and servers reduce the potential harm should any subsystem be compromised.
- ▶ **Redundancy:** Another key architectural control is redundancy, allowing a function to be performed on more than one node. Instead of having a single web server; a better design would have two servers,

using a “failover mode”. In failover mode, the servers communicate with each other periodically, each determining if the other is still active. If one fails, the other takes over processing for both of them. Although performance is cut approximately in half when a failure occurs, some minimum processing is being done which can be used to maintain critical functions.

- ▶ **Eliminating Single Points of Failure:** One way in which the architecture of a network can improve network security is to eliminate single points of failure. That is any single point in the network that, if it were to fail, could deny access to all or a significant part of the network. For example, a single database in one location is vulnerable to all the failures that could affect that location. Good network design eliminates single points of failure.

Cryptography/Encryption

The technical details of cryptography have been dealt with in an earlier module. Only certain applications of cryptography that are relevant to Network security are discussed here.

Link Encryption

In link encryption, data are encrypted just before the system places them on the physical communications link, that is, encryption occurs at the Data Link layer in the OSI model. Correspondingly, decryption occurs at the Data Link layer of the receiving host. (Note that according to some authors, the link encryption occurs at the physical layer).

Link encryption protects the message in transit between two computers, but the message is in plaintext inside the hosts (above the data link layer). Headers added by the network layer (which includes addresses, routing information and protocol) and above are encrypted, along with the message/data. The message is, however, exposed at the Network layer and thus all intermediate nodes through which the message passes can read the message. This is because all routing and addressing is done at the Network layer. Link encryption is invisible to the user, and appropriate when the transmission line is the point of greatest vulnerability. Link encryption provides protection against traffic analysis.

End-to-End Encryption

End-to-end encryption provides security from one end of a transmission to the other. The encryption can be applied by a hardware device between the user and the host or the encryption can be done by software running on the host computer. In either case, the encryption is performed at the higher layers, usually transport layer. (Note that according to [different] authors, end-to-end encryption can be done at presentation or application layer). When end-to-end encryption is used, messages, even when sent through several insecure intermediate hosts,

Module 3, Chapter 5

are protected. This is because the data content remains encrypted at all the intermediate layers. However, since the headers below the transport are not encrypted (networks, data link, etc.) end-to-end does not provide protection against traffic analysis.

Note that it is possible use both Link and End-to-end encryption at the same time. One does not preclude the other.

PKI and Certificates

A public key infrastructure (PKI) is a process created to enable users to implement public key (asymmetric) cryptography, usually in a large and distributed setting. PKI offers each user a set of services, related to identification and access control, as follows:

- ▶ Create certificates associating a user's identity with a (public) cryptographic key
- ▶ Issue certificates from its database
- ▶ Sign certificates, adding its credibility to the authenticity of the certificate
- ▶ Confirm (or deny) the validity of a certificate
- ▶ Revoke certificates for users who no longer are allowed access or whose private key has been exposed

PKI is a set of policies, procedures and products and not a standard. The policies define the rules under which the cryptographic systems should operate. In particular, the policies specify how to handle keys and valuable information and how to match level of control to level of risk. The procedures dictate how the keys should be generated, managed, and used. Finally, the products actually implement the policies, and they generate, store, and manage the keys. Entities, called certificate authorities, implement the PKI policy on certificates. The functions of a certificate authority can be done in-house or by a commercial service or a trusted third party. PKI also involves a registration authority that acts as an interface between a user and a certificate authority. The registration authority captures and authenticates the identity of a user and then submits a certificate request to the appropriate certificate authority.

SSL Encryption

The SSL (Secure Sockets Layer) protocol was originally designed by Netscape to protect communication between a web browser and server. It is also known now as TLS, for transport layer security. SSL interfaces between applications (such as browsers) and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communications channel between client and server.

To create a SSL connection, the client requests an SSL session. The server responds with its public key certificate so that the client can determine the authenticity of the server. The client returns symmetric ses-

sion key encrypted under the server's public key. The server decrypts the session key and then they switch to encrypted communication, using the shared session key.

IPSec

As a part of the IPv6 (version 6 of the IP protocol suite) suite, the IETF (Internet Engineering Task Force) adopted IPSec, or the IP Security Protocol Suite. Designed to address shortcomings in IPv4, such as being subject to spoofing, eavesdropping, and session hijacking, the IPSec protocol defines a standard means for handling encrypted data. IPSec is implemented at the IP layer, so it affects all layers above it, in particular TCP and UDP.

IPSec is similar to SSL, in that it supports authentication and confidentiality in a way that does not necessitate significant change either above it (in applications) or below it (in the TCP protocols). Like SSL, it was designed to be independent of specific cryptographic protocols and to allow the two communicating parties to agree on a mutually supported set of protocols.

Signed Code

As already noted, it is possible for someone to place malicious active code on a web site to be downloaded by unsuspecting users. A partial solution to reduce this risk is to use signed code. A trustworthy third party appends a digital signature to a piece of code (or macro), supposedly connoting more trustworthy code. A signature structure in a PKI helps to validate the signature. A well-known manufacturer would be recognizable as a code signer.

In this context, it is worth noting that in March 2001, Verisign (a certifying authority) announced it had erroneously issued two code-signing certificates under the name of Microsoft Corporation to someone who falsely claimed to be a Microsoft employee. These certificates were in circulation for almost two months before the error was detected.

Encrypted E-Mail

An electronic mail message generally has no privacy at all. The service provider and any intermediate host can read not just the address but also everything in the message field. To protect the privacy of the message and routing information, we need encryption to protect the confidentiality and integrity of the message. The two popular approaches to key management are using a hierarchical, certificate-based PKI solution for key exchange and using a flat, individual-to-individual exchange method. The hierarchical method is called S/MIME (Secure Multi Purpose Mail Extensions) and is employed by many commercial mail programs, such as Microsoft Exchange. The individual method is called PGP (Pretty Good Privacy) and is a commercial add-on.

Content Integrity

Content integrity is automatically implied when cryptographic systems are used. Most kinds of malicious threats are addressed by cryptographic systems very effectively. For non-malicious threats to integrity, the controls are Error Correcting codes and Message Digests (Cryptographic Checksums)

Error Correcting Codes

Error detection codes detect when an error has occurred, and error correction codes can actually correct errors without requiring retransmission of the original message. The error code is transmitted along with the original data, so the recipient can re-compute the error code and check whether the received result matches the expected value.

- ▶ **Parity Check:** The simplest error detection code is a parity check. An extra bit (the parity bit) is added to an existing group of data bits depending on their sum. With even parity the extra bit is 0 if the sum of the data bits is even and 1 if the sum is odd; that is, the parity bit is set so that the sum of all data bits plus the parity bit is even. Odd parity is the same except the sum is odd. Parity bits are useful only when the error is in a single bit (called single bit error).
- ▶ **Checksum and CRCs:** A checksum is a form of redundancy check, that at its simplest, works by adding up the basic components of a message, usually the bits or bytes, and storing the resulting value. Later, anyone who has the authentic checksum can verify that the message was not corrupted by doing the same operation on the data, and checking the sum. A more sophisticated type of redundancy check is the cyclic redundancy checks(CRC) which considers not only the value of each bit/byte but also the order of the values. A cyclic redundancy check (CRC) uses a hash function used to produce a checksum which is a small integer from a large block of data, such as network traffic or computer files, in order to detect errors in transmission or duplication. CRCs are calculated before and after transmission or duplication, and compared to confirm that they are the same.
- ▶ **Other Codes:** Other kinds of error detection codes, such as hash codes and Hamming codes are used to detect burst errors (several errors occurring contiguously) and multiple bit errors (multiple errors among non-adjacent bits). Some of the more complex codes (like Hamming codes) can detect multiple-bit errors and may be able to pinpoint which bits have been changed, thus allowing the data to be corrected.

Message Digests (Cryptographic Checksums)

Checksums and CRCs are useful in detecting accidental modification such as corruption to stored data or errors in a communication chan-

nel. However, they provide no security against malicious agents, as their simple mathematical structure makes them trivial to circumvent. To protect against malicious changes cryptographic checksums are used.

A cryptographic checksum is created by performing a complicated series of mathematical operations (the cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as a checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum.

A cryptographic hash function must ensure that the following is computationally infeasible:

- ▶ Determining the content of a message from its Cryptographic Checksums
- ▶ Finding “collisions”, wherein two different messages have the same Cryptographic Checksums.

Cryptographic checksums are also known as message digests, message authentication codes, integrity check-values, modification detection codes, or message integrity codes.

Strong Authentication

A security policy specifies who—which individuals, groups, subjects—can access which resources and objects. Crucial to that policy is authentication: knowing and being assured of the accuracy of identities. The authentication methods appropriate for use in networks are one-time passwords, Challenge Response systems and Kerberos.

- ▶ **One Time Passwords:** A one-time password can guard against wiretapping and spoofing of a remote host. In the simplest case, the user and host both have access to identical lists of passwords. The user would enter the first password for the first login, the next one for the next login, and so forth. As long as the password lists remained secret and as long as no one could guess one password from another, a password obtained through wiretapping would be useless. A more complex but practical implementation uses a password token, a device that generates a password that is unpredictable but that can be validated on the receiving end. The simplest form of password token is a synchronous one. This device displays a random number, generating a new number every minute. Each user is issued a different device (that generates a different key sequence). The user reads the number from the device's display and types it in as a one time password. The computer on the receiving end executes the algorithm to generate the password appropriate for the current minute; if the user's password matches the one computed remotely, the user is authenticated.

- ▶ **Challenge Response Systems:** A challenge and response device looks like a pocket calculator. The user first authenticates to the device, usually by means of a PIN. The remote system sends a random number, called the “challenge” which the user enters into the device. The device responds to challenge with another number, which the user then transmits to the system.
The system prompts the user with a new challenge for each use. Thus, this device eliminates the small window of vulnerability in which a user could reuse a time-sensitive authenticator. A generator that falls into the wrong hands is useless without the PIN.
- ▶ **Kerberos:** Kerberos is a system that supports authentication in distributed systems. Originally designed to work with secret key encryption, Kerberos, in its latest version, uses public key technology to support key exchange. Kerberos is used for authentication between intelligent processes, such as client-to-server tasks, or a user’s workstation to other hosts. Kerberos is based on the idea that a central server provides authenticated tokens, called tickets, to requesting applications. A ticket is an unforgeable, nonrepayable, authenticated object. That is, it is an encrypted data structure naming a user and a service that user is allowed to obtain. It also contains a time value and some control information.

Remote Access Security

Remote access technologies can be defined as those data networking technologies that are focused on providing the remote user with access into a network, while striving to maintain the principal tenets of Confidentiality, Availability, and Integrity.

There are many obvious advantages to employing secure remote network access, such as the following:

- ▶ Reducing networking costs by using the Internet to replace expensive dedicated network lines
- ▶ Providing employees with flexible work styles such as telecommuting
- ▶ Building more efficient ties with customers, suppliers, and employees

Virtual Private Networking (VPN)

A virtual private network (VPN) is created by building a secure communications link between two nodes by emulating the properties of a point-to-point private link. A VPN can be used to facilitate secure remote access into a network, securely connect two networks together, or create a secure data tunnel within a network. Encryption coupled with access controls (including firewalls) can provide users with the same level of privacy that can be provided on a private network, even when

the communication traverses a part of the public network. For more details, refer the previous module.

Dial back procedures

In a networked computing environment, user may often require access the systems resources from remote locations. Dial-back systems are a control to ensure that access is made only from authorised lines or locations. When a user dials into the server and identifies himself, the server hangs up and calls the user at a pre-determined telephone number and then enables the user to access the resources based on password authentication. A weakness in this procedure is call-forwarding. An unauthorized person could enable calls to a pre-determined number to be forwarded to the number designated by him, thus enabling him to gain unauthorized access to the resources.

Other controls

To minimize the risk of unauthorized dial-in access, remote users should never store their passwords in plain text login scripts on notebooks and laptops.

Authentication Servers

In widely spread out networked systems, the problems of user management and enabling authorised access is crucial since users dispersed over a wide geographical areas including tele-commuting. In such cases all access control is transferred to a centralized or decentralized access authentication servers. Two of the popular applications of remote authentication mechanisms depending on centralized/decentralized access authentication implementations are TACACS (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial In User Service). Some of the features of such systems are:

- ▶ Enable secure remote access
- ▶ Facilitates centralized user management
- ▶ Facilitates centralized access monitoring and control
- ▶ Changes to user access rights made easy
- ▶ Provides event logging and extended audit trails

Firewalls

The technical details of firewalls, their types and configurations have been dealt with in an earlier module, Module 2. Only certain specialised applications of firewalls for network security are dealt with here.

Virtual Private Networks

Firewalls and firewall environments are used to construct Virtual Private Networks (VPNs). See previous module for more details.

Intranet

An intranet is a network that employs the same types of services, applications, and protocols present in an Internet implementation, without involving external connectivity. For example, an enterprise network employing the TCP/IP protocol suite, along with HTTP for information dissemination would be considered an Intranet.

Most organizations currently employ some type of intranet, although they may not refer to the network as such. Within the internal network (intranet), many smaller intranets can be created by the use of internal firewalls. As an example, an organization may protect its personnel network with an internal firewall, and the resultant protected network may be referred to as the personnel intranet.

Since intranets utilize the same protocols and application services present on the Internet, many of the security issues inherent in Internet implementations are also present in intranet implementations. Therefore, intranets are typically implemented behind firewall environments.

Extranets

An extranet is usually a business-to-business intranet; that is, two intranets are joined via the Internet. The extranet allows limited, controlled access to remote users via some form of authentication and encryption such as provided by a VPN. Extranets share nearly all of the characteristics of intranets, except that extranets are designed to exist outside a firewall environment. By definition, the purpose of an extranet is to provide access to potentially sensitive information to specific remote users or organizations, but at the same time denying access to general external users and systems. Extranets employ TCP/IP protocols, along with the same standard applications and services. Many organizations and agencies currently employ extranets to communicate with clients and customers. Within an extranet, options are available to enforce varying degrees of authentication, logging, and encryption.

Securing a Firewall

Firewall platforms should be implemented on systems containing operating system builds that have been stripped down and hardened for security applications. Firewalls should never be placed on systems built with all possible installation options.

Firewall operating system builds should be based upon minimal feature sets. All unnecessary operating system features should be removed from the build prior to firewall implementation, especially compilers. All appropriate operating system patches should be applied before any installation of firewall components.

The operating system build should not rely strictly on modifications made by the firewall installation process. Firewall installation programs rely on a lowest common denominator approach; extraneous software packages or modules might not be removed or disabled during the installation process.

The hardening procedure used during installation should be tailored to the specific operating system undergoing hardening. Some often-overlooked issues include the following:

- ▶ Any unused networking protocols should be removed from the firewall operating system build. Unused networking protocols can potentially be used to bypass or damage the firewall environment. Finally, disabling unused protocols ensures that attacks on the firewall utilizing protocol encapsulation techniques will not be effective.
- ▶ Any unused network services or applications should be removed or disabled. Unused applications are often used to attack firewalls because many administrators neglect to implement default-restrictive firewall access controls. In addition, unused network services and applications are likely to run using default configurations, which are usually much less secure than production-ready application or service configurations.
- ▶ Any unused user or system accounts should be removed or disabled. This particular issue is operating system specific, since all operating systems vary in terms of which accounts are present by default as well as how accounts can be removed or disabled.
- ▶ Applying all relevant operating system patches is also critical. Since patches and hot fixes are normally released to address security-related issues, they should be integrated into the firewall build process. Patches should always be tested on a non-production system prior to rollout to any production systems.
- ▶ Unused physical network interfaces should be disabled or removed from the server chassis.

Intrusion Detection Systems

After the perimeter controls, firewall, and authentication and access controls block certain actions, some users are admitted to use a computing system. Most of these controls are preventive, that is, they prevent known undesirable things from happening. Many studies, however, have shown that most computer security incidents are caused by insiders, people who would not be blocked by a firewall. And insiders require access with significant privileges to do their daily jobs.

Intrusion detection systems complement these preventive controls as the next line of defence. An intrusion detection system (IDS) is a device, usually another separate computer, that monitors activity to identify malicious or suspicious events. An IDS is a sensor, that raises an alarm

Module 3, Chapter 5

if specific things occur. The alarm can range from writing an entry in an audit log, to something significant, such as paging the system security administrator.

An IDS receives inputs from sensors. It saves those inputs, analyzes them, and takes some controlling action. The functions performed by an IDS are:

- ▶ Monitoring users and system activity
- ▶ Auditing system configuration for vulnerabilities and mis-configurations
- ▶ Assessing the integrity of critical system and data files
- ▶ Recognizing known attack patterns in system activity
- ▶ Identifying abnormal activity through statistical analysis
- ▶ Managing audit trails and highlighting user violation of policy or normal activity
- ▶ Correcting system configuration errors
- ▶ Installing and operating traps to record information about intruders
- ▶ Special considerations in audit of remote access and network security

Many intrusion detection systems are also capable of interacting with firewalls in order to bring a reactive element to the provision of network security services. Firewalls that interact with intrusion detection systems are capable of responding to perceived remote threats automatically, without the delays associated with a human response. For example, if an intrusion detection system detects a denial of service attack in progress, it can instruct certain firewalls to automatically block the source of the attack (although, false positives responses can occur).

The two general types of intrusion detection systems are signature based and heuristic. Signature-based intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type. Heuristic intrusion detection systems, also known as anomaly based, build a model of acceptable behaviour and flag exceptions to that model; for the future, the administrator can mark a flagged behaviour as acceptable so that the heuristic IDS will now treat that previously unclassified behaviour as acceptable.

Intrusion detection devices can be network based or host based. A network-based IDS is a stand-alone device attached to the network to monitor traffic throughout that network; a host-based IDS runs on a single workstation or client or host, to protect that one host. For more details, please see the previous module.

Auditing Network Security

Auditing networked computing environments presents significant complexities. Networking enables several virtual machines to operate

together using a limited set of systems resources, irrespective of the barriers of geographic location of the user and systems infrastructure. For example, a customer can now access his bank account from anywhere in the world. This means that logical paths open up enabling access through insecure networks and diverse computing infrastructures.

Audit of network security requires the auditor to take special considerations into account and plan accordingly to achieve his audit objectives. The considerations while auditing network security are:

- ▶ Locating logical access paths by reviewing network diagrams to identify network topologies, virtual paths spanning across LANs, WANs and the open networks such as shared networks and the Internet.
- ▶ Recognizing logical access threats, risks and exposures in the networked environment.
- ▶ Identifying and controlling over access paths used for distributed processing and distributed databases.
- ▶ Evaluating network management and change control in respect of technical components such as modems, switches, routers, firewalls, VPNs, network management and access control software, encryption, protocols, middleware controls and Internet security.
- ▶ Identifying information resource owners can be quite complex since in a distributed computing environment, an application process can span several systems and networks, including those outside the organisation's control.
- ▶ Evaluating logical network security policies and practices.
- ▶ Evaluating effectiveness of logical access security with respect to network security components such as:
 - ▶ Firewalls and filtering routers - architecture, configuration setting as per firewall security policy, port services, anti-virus configuration, reporting and management controls
 - ▶ Intrusion detection systems - architecture, configuration, interface with other security applications, reporting and management controls
 - ▶ Virtual private networks - architecture, devices, protocol, encryption process integration with firewall security, change management
 - ▶ Security protocols - selection of appropriate protocol, seamless security integration of protocols between devices running different protocols
 - ▶ Encryption - selection of appropriate encryption methods to various application processes
 - ▶ Middleware controls - middleware design and access control with respect to identification, authentication and authorisation, management of components and middleware change management.
- ▶ Network event logging and monitoring

Penetration Testing

Introduction

Adequately protecting an organization's information assets is a business imperative – one that requires a comprehensive, structured approach to provide protection commensurate with the risks an organization might face. The purpose of this section is to explore an ethical hacking technique – referred to in the IT community as Penetration Testing – that organizations are increasingly using to evaluate the effectiveness of information security measures.

As its name implies, penetration testing is a series of activities undertaken to identify and exploit security vulnerabilities. The idea is to find out how easy or difficult it might be for someone to “penetrate” an organization's security controls or to gain unauthorized access to its information and information systems.

A penetration test typically involves a small team of people sponsored by the organization asking for the test. This team attempts to exploit vulnerabilities in the organization's information security by simulating an unauthorized user (or “hacker”) attacking the system using similar tools and techniques. Penetration testing teams typically comprise people from an organization's Internal Audit department or IT department, or from consulting firms specializing in these types of services. Their goal is to attempt to identify security vulnerabilities under controlled circumstances, so that they can be eliminated before unauthorized users can exploit them. Because penetration testing is an authorized attempt to simulate hacker activities, it is often referred to as “ethical hacking.”

It is important to point out that a penetration test cannot be expected to identify all possible security vulnerabilities, nor does it offer any guarantee that an organization's information is secure. Penetration testing is typically conducted at a point in time. New technology, new hacker tools and changes to an organization's information system can create exposures not anticipated during the penetration testing. In addition, penetration testing is normally completed with finite resources, focused on a particular area, over a finite period of time. Hackers determined to break into an organization's information systems are often not bound by similar constraints. Penetration testing is also typically focused on a system's security vulnerabilities that would enable unauthorized access. It is not necessarily focused on security vulnerabilities that could result in the accidental loss or disclosure of the organization's information and information systems.

Many organizations have deployed sophisticated security mechanisms, such as firewalls or intrusion detection systems (IDS), to help protect their information assets and to quickly identify potential attacks. While

these mechanisms are important, they are not foolproof. A firewall cannot protect against what is allowed through – such as online applications and allowed services. While an IDS can detect potential intrusions, it can detect only what it has been programmed to identify, and it will not be effective at all if the company does not monitor or respond to the alerts. Also, firewalls and intrusion detection systems must be continuously updated or they risk losing their effectiveness at preventing or detecting attacks. Penetration testing can help validate and confirm the effective configuration of an organization's firewalls and its intrusion detection systems.

Penetration Testing Scope

The scope of a penetration testing project is subject to negotiation between the sponsor of the project and the testing team, and will vary depending on the particular objectives to be achieved. The principal objective of penetration testing is to determine whether an organization's security vulnerabilities can be exploited and its systems compromised.

Conducting such a test involves gathering information about an organization's information systems and information security and then using this information to attempt to identify and exploit known or potential security vulnerabilities. Evidence to support the penetration testing team's ability to exploit security vulnerabilities can vary from gathering "computer screen shots" or copying sensitive information or files to being able to create new user accounts on the system or being able to create and/or delete particular files on the organization's servers.

Penetration testing can have a number of secondary objectives, including testing the security incident identification and response capability of the organization, testing employee security awareness or testing users' compliance with security policies. There are two areas that should be considered when determining the scope and objectives of a penetration testing exercise: testing strategies and testing activities to be executed.

Penetration Testing Strategies

Various strategies for penetration testing, based on specific objectives to be achieved, include:

- ▶ **External vs. internal testing.** External testing refers to attacks on the organization's network perimeter using procedures performed from outside the organization's systems, that is, from the Internet or Extranet. To conduct the test, the testing team begins by targeting the company's externally visible servers or devices, such as the Domain Name Server (DNS), email server, web server or firewall. Internal testing is performed from within the organization's technology environment. The focus is to understand what could happen if the network perimeter were successfully penetrated or what an au-

thorized user could do to penetrate specific information resources within the organization's network.

- ▶ **Blind and double blind vs. targeted testing strategy.** In a blind testing strategy, the testing team is provided with only limited information concerning the organization's information systems configuration. The penetration testing team must use publicly available information (such as company web-site and domain name registry, Internet discussion board) to gather information about the target and conduct its penetration tests. Blind testing can provide information about the organization that may have been otherwise unknown, but it can also be more time consuming and expensive than other types of penetration testing (such as targeted testing) because of the effort required by the penetration testing team to research the target.
- ▶ **Double-blind testing** extends the blind testing strategy in that the organization's IT and security staff are not notified or informed beforehand and are "blind" to the planned testing activities. Double-blind testing can test the security monitoring and incident identification of the organization, escalation and response procedures. Normally, in double-blind testing engagements, very few people within the organization are made aware of the testing, perhaps only the project sponsor. Double-blind penetration testing requires careful monitoring by the project sponsor to ensure that the testing procedures and the organization's incident response procedures can be terminated when the objectives of the test have been achieved.
- ▶ **Targeted testing** (often referred to as the "lights-turned-on" approach) involves both the organization's IT team and the penetration testing team being aware of the testing activities and being provided information concerning the target and the network design. A targeted testing approach may be more efficient and cost-effective when the objective of the test is focused more on the technical setting, or on the design of the network, than on the organization's incident response and other operational procedures. A targeted test typically takes less time and effort to complete than blind testing, but may not provide as complete a picture security vulnerabilities and response capabilities of the organization.

Types of Penetration Testing

In addition to the penetration testing strategies to be used, consideration should be given to the types of testing the testing team is to carry out. These could include:

- ▶ **Application security testing.** Many organizations offer access to core business functionality through web-based applications. This type of access introduces new security vulnerabilities, because even with a firewall and other monitoring systems, security can be compromised, since traffic must be allowed to pass through the firewall. The

objective of application security testing is to evaluate the controls over the application and its process flow. Areas of evaluation may include the application's usage of encryption to protect the confidentiality and integrity of information, how users are authenticated, integrity of the Internet user's session with the host application, and use of cookies – a block of data stored on a customer's computer that is used by the web server application.

- ▶ **Denial of Service (DoS) testing.** The goal of DoS testing is to evaluate the system's susceptibility to attacks that will render it inoperable so that it will “deny service,” that is, drop or deny legitimate access attempts. Decisions regarding the extent of Denial of Service testing to be incorporated into a penetration testing exercise will depend on the relative importance of ongoing, continued availability of the information systems and related processing activities.
- ▶ **War Dialing.** War dialing is a technique for systematically calling a range of telephone numbers in an attempt to identify modems, remote access devices and maintenance connections of computers that may exist on an organization's network. Well-meaning users can inadvertently expose the organization to significant vulnerability by connecting a modem to the organization's information systems. Once a modem or other access device has been identified, analysis and exploitation techniques are performed to assess whether this connection can be used to penetrate the organization's information systems network.
- ▶ **Wireless network penetration testing.** The introduction of wireless networks, whether through formal, approved network configuration management or the inadvertent actions of well-meaning users, introduce additional security exposures. Sometimes referred to as “war-driving,” hackers have become proficient in identifying wireless networks simply by “driving” or walking around office buildings with their wireless network equipment. The goal of wireless network testing is to identify security gaps or flaws in the design, implementation or operation of the organization's wireless network.
- ▶ **Social Engineering.** Often used in conjunction with blind and double-blind testing, this refers to techniques using social interaction, typically with the organization's employees, suppliers and contractors, to gather information and penetrate the organization's systems. Such techniques could include:
 - ▼ posing as a representative of the IT department's help desk and asking users to divulge their user account and password information;
 - ▼ posing as an employee and gaining physical access to restricted areas that may house sensitive information;
 - ▼ intercepting mail, courier packages or even trash to search for sensitive information on printed materials.

Social engineering activities can test a less technical, but equally important, security component: the ability of the organization's people to contribute to, or prevent, unauthorized access to information and information systems.

Risks associated with Penetration Testing

While management sponsors the testing activities, those activities do, in themselves, represent some level of risk. Some of the key risks include the following:

- ▶ the penetration test team may fail to identify significant vulnerabilities;
- ▶ misunderstandings and miscommunications may result in the test objectives not being achieved;
- ▶ testing activities may inadvertently trigger events or responses that may not have been anticipated or planned for (such as notifying law enforcement authorities);
- ▶ sensitive security information may be disclosed, increasing the risk of the organization being vulnerable to external attacks.

During the course of the penetration testing, significant security vulnerabilities can, and likely will be, identified. Such information must be adequately protected to minimize the risk that it does not create a further security exposure by falling into the wrong hands.

Some questions to consider include:

- ▶ Will activities be conducted over the Internet or other public network? If so, how is information protected while in transmission over such networks?
- ▶ How and where will information that is collected, including working paper files, be stored? In electronic form? In physical form? Who has, or will have, custody of this information, including summaries of findings and observations?
- ▶ How much information will the final reports and executive summaries contain? How will content and distribution of findings, observations and reports be controlled?
- ▶ How will notes, working papers and other forms of information be retained or destroyed?
- ▶ Do the terms of engagement include appropriate provisions to protect the confidentiality of the information collected, as well as the findings, observations and recommendations?

Defining when testing activities end. The activities or events that will trigger the conclusion of the penetration testing activities should be clearly described in the engagement scope definition. Such activities or events would, of course, depend on the specific objectives of the test, but could, for example, include collecting proof of the team's ability to exploit security vulnerabilities. This "proof" could take many forms, such

as copying a target file, creating a file on a target server, adding a new user to a target system or capturing “screen shots” of a target application system. In some instances, it may be appropriate to define a time period within which the testing is to be completed.

Network Infrastructure Auditing Checklist

The following is a general illustrative checklist for the audit of Network infrastructure.

Network Server

- Obtain or prepare logical and physical diagrams of the network and attached local and wide area networks, including the systems’ vendor and model description, physical location, and applications and data residing and processing on the servers and workstations.
- Using the information obtained in the prior steps, document the server and directory location of the significant application programs and data within the network; document the flow of transactions between systems and nodes in the network.
- Assess whether the trusted domains are under the same physical and administrative control and are logically located within the same sub-network.
- Determine that router filtering is being used to prevent external network nodes from spoofing the IP address of a trusted domain.
- Determine that the Administrator/superuser and Guest accounts have passwords assigned to them (by attempting to log on without providing a password). Also ascertain that the Administrator account password is well controlled and used/know by only the system administrator and one backup person.
- Review the account properties settings active in each user’s individual profile, which may override the global account policy.
- List out the security permissions for all system directories and significant application programs and directories and ensure that they are consistent with security policy
- Review and assess permissions assigned to groups and individual accounts, noting that Full Control (all permissions) and Change (Read, Write, Execute, and Delete) permissions are restricted to authorized users.
- Review the audit log for suspicious events and follow up on these events with the security administrator.

Router

- Determine the types of accounts that were used to access the routers.
- Determine what users had access to these accounts.
- Were access attempts to the routers logged?

Module 3, Chapter 5

- Determine if all accounts had passwords and determine the strength of the passwords.
- Was simple network management protocol (SNMP) used to configure the network?
- Determine the version of SNMP employed by the Company. (Version one stores passwords in clear-text format. Version two adds encryption of passwords.)
- Determine if open shortest path first (OSPF) was defined on the router. Determine the authentication mechanism that was employed in the Company's implementation of OSPF.
- Determine whether directed broadcast functionality was enabled on the router. This setting, if enabled, could allow a denial-of-service (DoS) attack of the network (Smurf attack).
- Obtain population of routers with modems and obtain the telephone numbers of the routers.
- Determine if users were properly authenticated when remotely accessing the routers.
- Determine how changes to the router environment were made. Were there procedures for changing router configurations? If so, were these procedures well-documented and consistent with security policy?
- Determine if changes to the router configuration were documented.
- Was there a separation of duties within the change control of the router environment?

Firewalls

- Obtain background information about the firewall(s), in place, e.g., segment diagrams, software, hardware, routers, version levels, host names, IP addresses, connections, any specific policies for an overview of the firewall security
- Determine that the firewall components, both logical and physical, agree with the firewall strategy.
- Determine whether the firewall components are the latest possible version and security patches are current.
- Determine that the root cannot telnet to the system.
- Determine the telnet OS banner and other banners such as FTP banner, etc. has been eliminated.
- Ensure that there are no compilers/interpreters on the firewall.
- Ensure that a lockdown rule has been placed at the beginning of the rule base. The lockdown rule protects the firewall, ensuring that whatever other rules are put in later, it will not inadvertently compromise the firewall.
- Obtain and review the connections table for time out limits and number of connections
- Attempt to test the rule base by scanning secured network segments from other network segments

- ▶ Identify accessible resources behind the firewall that are to be encrypted and determine the connections are encrypted
- ▶ Determine if there is a change control process in place for the rule base
- ▶ Determine the use of the firewall's automatic notification/alerting features and archiving the detail intruder information to a database for future analysis.

Network Administration and Security Auditing Checklist

The following is a general checklist for the audit of Network Administration and Security.

Process

- ▶ Is there an Information Security guidelines document, which defines the minimum configuration for any device/link on the organisation's network, including levels of encryption?
- ▶ Are all platforms/links/devices in compliance with the guidelines? If not, has an appropriate level of management reviewed the non-compliant parts of the network to ensure that the risk levels are acceptable?
- ▶ For all items supported by external vendors, does the vendor or the manufacturer verify that all cryptographic functions in use by the product/service, such as encryption, message authentication or digital signatures, use approved cryptographic algorithms and key lengths.
- ▶ Wherever applicable, whether background and reference checks for both internal and outsourced vendor staff who perform security-related functions for the product/service under review are carried out. This includes job applicants who have accepted a job offer, temporaries, consultants, full time staff as well as the outsourced vendor who is involved in product/service management and operations.

Authentication

- ▶ Does the product/service authenticate (verify) the identity of users (or remote systems) prior to initiating a session or transaction? Have these authentication mechanisms been approved by then organization's IT Department? (These include Passwords, Personal Identification Numbers (PINs), (static and dynamic), public keys and biometrics.)
- ▶ Does the organization verify that the initial authentication has used a mechanism that is acceptable for the application? Has the approach been approved by IT Department and required compensating controls have been implemented?
- ▶ Does the organisation have a comprehensive password construction, implementation and management policy?
- ▶ Do the Products/Services utilizing biometrics authentication only use biometrics for local authentication?

Public Key Infrastructure (PKI)

- Do the Products/services using Public key (or asymmetric) cryptography for authentication either on a session basis (peer authentication) or on a per-message/transaction basis (digital signatures) use approved security protocols to comply with the public key technology standard?
- For products/services that use PKI, private keys which are stored in hardware or software must be protected via an approved mechanism. The protection mechanism includes user authentication to enable access to the private key. Are these protections mechanisms adequate?
- For products/services that use PKI, an approved process for verifying the binding of a user identity to the public key (e.g., digital certificate) is required for any server relying on public key authentication. Is such a processes in place?

Access Control

- Is the access to highly privileged IDs (e.g., system administration access) strictly controlled, audited and limited in its use?
- Does the product/service support the need to perform a periodic entitlement review? A periodic entitlement review process should validate access privileges.
- Does the product/service support the requirement to limit individual user sessions to a maximum of X minutes of inactivity using either session time out or a password protected screen saver?
- Is there a process in place to ensure that access rights reflect changes in employee or job status within X hours of the change? This includes physical access tokens and dial-in capabilities as well as any systems or applications.
- For any products/services, which has been outsourced, is there a process in place to ensure that all platforms, services and applications are configured to meet organisation's Information Security Standards?
- Does the product/service display the (a) date and time of last successful login and (b) the number of unsuccessful login attempts since the last successful login?
- Does the product/service support a periodic process to ensure that all user IDs for employees, consultants, agents, auditors, or vendors are disabled after X days and deleted after Y days from the day they were not used unless explicitly approved by the concerned business manager.

Cryptography

- Is there a cryptography/encryption policy for various types of classified information that travels/gets stored within and outside the organisation's network(s)?

Network Information Security

- ▶ Is the approved Legal Affairs banner being displayed at all entry point where an internal user logs into the product/service? An automated pause or slow roll rate is in place to ensure that the banner is read. The Legal Affairs Banner usually carries the following kind of text:

“You are authorized to use this system for approved business purposes only. Use for any other purposes is prohibited. All transactional records, reports, e-mail, software and other data generated or residing upon this system are the property of the Company and may be used by the Company for any purpose. Authorized and unauthorized activities may be monitored.”

NOTE: This is required for all mainframe, mid-range, workstation, personal computer, and network systems.

- ▶ Has dial-in connectivity been prohibited on network-connected machine (server and workstation) except where documented and explicitly approved in writing by Business Management and the IT Department. When explicitly approved, the modem must, as a minimum control, prohibit answer or pickup until after the 5th ring.
- ▶ Have the remote control products used in a dial-in environment been approved by the IT Department explicitly?
- ▶ Is it ensured that only software (applications /operating systems, etc.) supported by the vendors are used? (Unsupported software could be vulnerable to attacks since the vendors would not come up with the relevant patches.)

Information Security Administration

- ▶ Is there an approved document clearly outlining the Security Administrator's (SA) responsibility?
- ▶ Are all the administrative actions (e.g., adding/deleting users, changes to entitlements/passwords) backed up by an independent review?
- ▶ Does the Security Administrator function review all security audit logs, incident reports, and on-line reports at least once per business day?
- ▶ In case of Wide Area Networks (WAN), are the router tables maintained securely in Routers?
- ▶ Are router login IDs and passwords treated as sensitive information and managed by authorised administrators?
- ▶ Are all changes to router table entries logged and reviewed independently? Are access violations taken note of, escalated to higher authority and acted upon in a timely manner?
- ▶ Is there a process to report all unusual or suspicious activity? (Reporting to IT Department, investigating immediately, and bringing the case to closure without delay)?

Module 3, Chapter 5

- Does the Security Administrator function assess compliance with their security procedures quarterly and reports their results to the IT Department?
- Have all the all security related administrative procedures under the control of the Security Administrator been documented and approved by management (annual exercise)? At minimum procedures should include:
 - ▼ Information Ownership
 - ▼ Data Classification
 - ▼ User registration/Maintenance
 - ▼ Audit Trail review
 - ▼ Violation logging and reporting
 - ▼ Sensitive activity reporting
 - ▼ Semi-Annual Entitlement Reviews
 - ▼ Password resets
 - ▼ ‣ Escalation reporting

Microcomputer/PC Security

- Does the LAN servers, mail servers, and microcomputers have IT Department approved anti-virus products installed?
- Are all product/service specific microcomputers/PCs secured against removal and theft commensurate with the value of the computer and information it holds along with a process to report any thefts to the IT Department?
- Are microcomputers / PCs having sensitive information protected with power-on password to prevent unauthorized access?
- Are sensitive data in such microcomputers / PCs backed up and preserved properly to ensure recovery in case of failure?

Audit Trails

- Does the audit trail associate with the product/service support the ability to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, highly privileged accounts and emergency IDs?
- Does the financial transactions as well as additions, changes and deletions to customer's and vendor's data, get recorded in the product/service audit trail?
- Does the audit trail for product/service record all identification and authentication processes? Also is there a retention period for the audit trails? Is it adequate?
- Does the audit trail associate with the product/service log all actions by the Security Administrator?
- Is there a process to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, security administrators, and highly privileged IDs?

- ▶ Is there a process in place to log and review actions performed by emergency IDs associated with the product/service?

Violation Logging Management

- ▶ Whether the product/service is capable of logging the minimum criteria specified to log and report specific security incidents and all attempted violations of system integrity
- ▶ Are the product/service owners aware of their responsibilities with respect to Security incident reporting?

Information Storage And Retrieval

- ▶ Has all the media (File/Floppy/Disks/Tapes etc) under the control of the product/service owner been marked with the classification and securely stored with access restricted to authorized personnel only?
- ▶ Is there a process in place to ensure that all media under the control of the product/service owner containing critical information is destroyed in a manner that renders the data unusable and unrecoverable?
- ▶ Is there a procedure in place that enforces and maintains a clean desk program, which secures all critical information from unauthorized access?

Penetration Testing

- ▶ Is it ensured that products/services that use the Internet for connectivity or communications have undergone a successful penetration test prior to production implementation?
- ▶ Is there a penetration test process that ensures whether modifications to the product/service that uses the Internet for connectivity or communication have been reviewed to determine whether a subsequent penetration test is warranted?
- ▶ Is there an intrusion detection system in place for all the external IP connections?

Summary

A network in its simplest form, is two devices connected across some medium by hardware and software that enable communication. Real-world corporate networks are significantly more complex and critical to performing business functions. These networks are vulnerable to a wide range of threats that could compromise the confidentiality, integrity, or availability of data, software and hardware by accidents, non-malicious humans, and malicious attackers.

To counter these threats there are various network security controls that are available to protect networks security from the various threats. There controls are include Network Architecture, Cryptography/

Module 3, Chapter 5

Encryption, Content Integrity measures, Strong Authentication, Remote Access Security, Firewalls, Intrusion Detection Systems.

Cryptography provides for security of data while in transit between two systems. Cryptographic systems are also used for authentication, in the form of digital signatures which are used to authenticate messages. These systems provide for confidentiality, integrity and authentication of messages.

Firewalls are mechanisms to enforce access control systems. They are the tools through which an organisation enforces its access control policy. Intrusion detection systems are tools to detect and monitor attempts to break into protected network. Firewalls and intrusion detection systems usually complement each other.



6 Securing Physical Access

✂ Learning Goals ✂

To understand:

- ▶ Physical access assets, threats and exposures
- ▶ Physical access controls and techniques of control
- ▶ Audit and evaluation of physical access

Introduction

Physical threats to Information System Assets include threats to computing equipment, facilities which house the equipment, media and people. This section deals with the security of the physical equipment and infrastructure and the environment in which they operate. The focus of the IS Auditor is to examine all factors that adversely bear on the confidentiality, integrity and availability of the information, due to improper physical access.

IS Assets: Objects of Physical Access Controls

In a computing environment, critical organisational information and data generally reside in electronic form in physical assets such as computing equipments or media and travel on communication lines.

A typical computing environment would house computers, numerous supporting computing equipments, communications equipment, and the like, facilities which house the computing equipment and infrastructure such as computer rooms, power sources, offsite storage. Further one would find storage media, documents, computer supplies, documentation related to Information Systems resources. Each of these information systems resources may need differing approaches to security both in terms of the techniques of securing them and appropriate investment to secure them. Hence the need to categorise such assets. From the perspective of physical access and control, Information Systems resources may be categorized as follows:

1. **Hardware and Media:** This includes computing equipment, peripherals, communication equipment and storage media. While the investment in the above tangible assets is usually significant, they assume even more significance depending on the type of content residing/under transmission in such devices. The content could include data, backups of data, application software and systems software.
- ▶ **Information Systems Supporting Infrastructure or Facilities:** Includes computer rooms, programming area, storage area, power sources, facili-

Module 3, Chapter 6

ties housing remote computing equipment, disposal sites, communication closet, off-site back-up areas.

- ▶ **Documentation:** IT plan, network documentation, systems documentation, programming documentation, database documentation, security deployment plan and technical manuals such as firewall documentation.
- ▶ **Supplies:** Blank pre-printed forms, cheque stationery, tapes, disks.
- ▶ **People:** Another critical component of a successful IPF (Information Processing Facility) is the personnel authorised and having rights of physical access to the above, such as database administrators, network engineers, analysts, programmers, console operators, data entry operators.

The above assets may be located across the physical premises of the organisation or outside the premises of the organisation. For example communication devices, shared devices and facilities, etc. may not be within the physical control of the organisation.

Physical Access Threats and Exposures

Threats from improper physical access usually are human-induced. Some illustrative examples are:

- ▶ Unauthorized persons gaining access to restricted areas. Examples are prospective suppliers gaining access to computer terminal of purchases department, thereby viewing list of authorized suppliers and rates being displayed on the screen during data entry.
- ▶ Employees gaining access to areas not authorized, e.g. sales executives gaining access to server room.
- ▶ Damage, vandalism or theft of equipments or other IS resources.
- ▶ Abuse of data processing resources, e.g. Employees using internet for personal purposes.
- ▶ Damage due to civil disturbances and war.
- ▶ Embezzlement of computer supplies, e.g. floppies, cartridges, printer consumables.
- ▶ Public disclosure of sensitive information, e.g. Information regarding location of servers, confidential or embarrassing information.

Improper physical access to IS resources may result in losses to organisation which can result in one or any of the following:

- ▶ Compromising confidentiality of organisational information or knowledge of protected organisational resources. Example: unauthorized access to systems containing sensitive information may be viewed or copied by visitors accidentally gaining access to such systems.

- ▶ Compromising integrity of information by improper manipulation of information or data contained on systems or media. Example: Unauthorized access to record rooms or databases may result in modification or deletion of file content.
- ▶ Compromising availability of information: Improper access to IS resources may be used to adversely impact availability of IS resources ultimately preventing or delaying access to organisational information and business applications. Example: A disgruntled bank employee may switch off power to information servers thus sabotaging operations.

Physical Access Exposures can also be classified as follows:

- ▶ Unintentional or Accidental: Authorised personnel or unauthorized personnel unintentionally gaining physical access to IS resources resulting in accidentally or inadvertently causing loss or damage to the organisation.
- ▶ Deliberate: Unauthorized personnel may deliberately gain access or authorised personnel may deliberately gain access to IS resources, in respect of which they are not permitted rights of access. This may result in the perpetrator achieving his objectives of causing loss or damage to organisation or the perpetrator gaining personally either monetarily or otherwise.

Sources of Physical Access Threats

The sources of physical access threats can be broadly divided into the following based on the nature of access:

- ▶ Physical access to IS resources by unauthorized personnel.
- ▶ Authorised personnel having pre-determined rights of access, mis-using their rights in a manner prejudicial to the interests of the organisation.
- ▶ Authorised personnel gaining access to Information Systems resources in respect of which they are not authorized access. (i.e. gaining access to resources beyond their rights of “need to know; need to do”)

The perpetrators or source of physical threats can be as follows:

- ▶ Interested or Informed outsiders such as competitors, thieves, organized criminals and hackers
- ▶ Former Employees
- ▶ Accidental Ignorant
- ▶ Discontented or disgruntled employees
- ▶ Employees on strike
- ▶ Employees under termination or suspended pending termination
- ▶ Addicted to substances or gamblers
- ▶ Experiencing financial or emotional problems

Physical Access Control Techniques

Physical Access controls seek to safeguard the IS resources from Physical Access exposures. However designing, acquiring and implementing controls is an expensive proposition. Risk Assessment provides the justification for the deployment of these physical access control techniques. Physical access controls encompass securing physical access to computing equipment as well as facilities housing the IS computing equipment and supplies etc. The choice of safeguard should be such that they prevent unauthorized physical access but at the same time cause the least inconvenience to authorized users.

Physical access controls may be broadly classified into administrative and technical controls. Give below are some of the means to control physical access:

Administrative Controls

Choosing and Designing a Secure Site

The location of the facility is also a concern that must be addressed during initial planning. The following considerations apply:

- ▶ **Natural disasters.** Probability of natural disasters as compared to other locations? Natural disasters can include weather-related problems (wind, snow, flooding, Tsunami and so forth) and earthquake faults.
- ▶ **Local considerations.** What is the local rate of crime (such as forced entry and burglary)?
- ▶ **Transportation.** Does the site have a problem due to excessive air, highway, or road traffic?
- ▶ **External services.** The relative proximity of the local emergency services, such as police, fire, and hospitals or medical facilities has to be factored in while choosing a site.

With respect to designing the site the following considerations apply:

- ▶ **Visibility.** Facilities such as data centres should not be visible or identifiable from the outside, that is, no windows or directional signs.
- ▶ **Windows.** Windows are normally not acceptable in the data centre. If they do exist, however, they must be translucent (or semi-transparent, i.e. allowing light without being able to view things clearly) and shatterproof.
- ▶ **Doors.** Doors in the computer centre must resist forcible entry and have a fire rating equal to the walls. Emergency exits must be clearly marked and monitored or alarmed. Electric door locks on emergency exits should revert to a disabled state if power outages occur to enable safe evacuation. While this may be considered a security issue, personnel safety always takes precedence, and these doors should be manned in an emergency.

Security Management

- ▶ **Controlled user registration procedure:** It should be ensured that rights of physical access are given only to persons entitled thereto and to the extent necessary, based on the principles of least privileges.
- ▶ **Audit Trails.** With respect to physical security, audit trails and access control log are vital because management needs to know where access attempts occurred and who attempted them. The audit trails or access logs must record the following:
 - ▼ The date-and time of the access attempt
 - ▼ Whether the attempt was successful or not
 - ▼ Where the access was granted (which door, for example)
 - ▼ Who attempted the access
 - ▼ Who modified the access privileges at the supervisor level
- ▶ **Reporting and incident handling procedure:** Once an unauthorized event is detected, appropriate procedures should be in place to enable reporting of such incidents and effectively handling such incidents to mitigate losses. The security administrator should be kept notified of such incidents. The security administrator may use such history to effect modifications to the security policy.

Emergency Procedures

The implementation of emergency procedures and the employee training and knowledge of these procedures is an important part of administrative physical controls. These procedures should be clearly documented, readily accessible (including copies stored off-site in the event of a disaster), and updated periodically.

Administrative Personnel Controls

Administrative personnel controls encompass those administrative processes that commonly are implemented by the Human Resources department during employee hiring and firing. These include pre-employment screening, ongoing employee checks, and post-employment procedures.

Technical Controls

These controls are not considered specifically administrative solutions, though they may have administrative aspects. Given below are various tools and technique to achieve physical security.

Guards: Guards are commonly deployed in perimeter control, depending on cost and sensitivity of resource to be secured. While guards are capable of applying subjective intelligence, they are also subject to the risks of social engineering. They are useful whenever immediate, discriminating judgment is required.

Module 3, Chapter 6

Dogs: Dogs are used in perimeter security. They are loyal, reliable, and have a keen sense of smell and hearing. However, they cannot make judgment calls the way humans can.

Compound walls and perimeter fencing: A common method of securing against unauthorized boundary access to the facility. It helps in deterring casual intruders but is ineffective against a determined intruder.

Lighting: Lighting is also one of the most common forms of perimeter or boundary protection. Extensive outside lighting of entrances or parking areas can discourage casual intruders.

Deadman Doors: Also called as Mantrap systems. These are typically used to secure entrance to sensitive computing facilities or storage areas. This technique involves a pair of doors and the space between the doors is enough to accommodate just one person. When a person is to be admitted to the premises, the second or inner door is closed while the first or outer door opens, thus admitting one person in the space between the doors. Once within that space the first door closes and then the second or inner door opens. Such doors reduce the risk of piggybacking, in which an unauthorized person could enter the secured facility by closely following an authorized person. It may or may not be monitored by a guard.

Bolting door locks: This is the most commonly used means to secure against unauthorized access to rooms, cabins, closets. These use metal locks and keys and access can be gained by any person having physical possession of the key. This is cheap yet a reasonably effective technique, however control over physical custody and inventory of keys is required.

Combination or Cipher locks: The most common kind of cipher lock consists of a push button panel that is mounted near the door outside of the secured area. There are ten numbered buttons on the panel. To gain entry, a person presses a four digit number in a particular pre-determined sequence which disengages the levers for a preset interval of time. Cipher locks are used where large number of entrances and exits must be usable frequently. Such locks (both cipher and combination) enable resetting the unlocking sequence periodically or as per requirement. One of the most common application of combination locks is the number locks on briefcases.

Electronic Door Locks: Such locks may use electronic card readers, smart cards readers or optical scanners. The readers or scanners read the cards and upon the information stored on the card matching with the information pre-stored internally in the reader device, the device disengages

the levers securing the door, thus enabling physical access. The advantages of such locks include:

- ▶ This technique provides a higher level of security over the previous discussed devices.
- ▶ The same device can be used to distinguish between various category of users.
- ▶ Individual access needs can be restricted through the special internal code and sensor devices. Restrictions can be assigned to particular doors or to particular hours.
- ▶ Duplication of such cards is difficult.
- ▶ Card entry can be easily deactivated from a central electronic control mechanism. This is useful in case of cards being lost or for disabling access to terminated employees etc. This also enables easy implementation of changes to security policy.
- ▶ The devices may also include various features such as “card swallow” after preset number of failed attempts, activating audible alarms, engaging other access areas thus securing sensitive areas or trapping the unauthorized entrant.
- ▶ However administrative control over card issue, access monitoring, securing electronic communication medium of the mechanism, access to device’s programming mechanism must be ensured for effective security.

Biometric Door Locks: These are some of the most secure locks since they enable access based on individual features such as voice, fingerprint, hand geometry, retina or iris. These are similar to the electronic door locks but more sophisticated since in this case the mechanical component securing the physical door is engaged/disengaged is controlled by an electronic device. In this case the device has a scanner/reader which reads the fingerprint or such other biometric and matching the individuals features with that internally stored. While these devices are considered highly secure, they suffer from the following disadvantages:

- ▶ Relatively high cost of acquisition, implementation and maintenance, hence they are used mainly to secure sensitive installations.
- ▶ Time consuming process of user registration.
- ▶ Privacy issues relating to use of devices like retina and fingerprint scanners.
- ▶ High error rates compared to other devices since they may result in a false rejection or more critically a false acceptance.

Video Cameras: Cameras provide preventive and detective control. Closed-Circuit Television (CCTV) cameras have to be supplemented by security monitoring and guards for taking corrective action. The location of such cameras and recording/retention of tapes/images for future playback should be decided based on security strategy.

Module 3, Chapter 6

Identification badges: Special identification badges such as employee cards, privileged access pass, visitor passes etc. enable tracking movement of personnel. These can also be cards with signature and/or photo identity. These are physically examined by security staff to permit/deny access and detect unauthorized access.

Manual Logging: All visitors to the premises are prompted to sign a visitor's log recording the date and time of entry/exit, name of entrant, organisation, purpose etc. The visitor may also be required to authenticate his identity by means of a business card, photo identification card, driver's licence etc.

Electronic Logging: As discussed in the previous section, electronic card users may be used to record the date and time of entry/exit of the card holder by requiring the person to swipe the card both time of entry and exit. This is a faster and more reliable method for restricting access to employees and pre-authorised personnel only. These devices may use electronic/biometric security mechanisms.

Controlled single point access: Physical access to the facility is granted though a single guarded entry point. Multiple entry points may dilute administration of effective security. This involves identifying and eliminating or disabling entry from all entry points except one.

Controlled Visitor access: A pre-designated responsible employee or security staff escorts all visitors such as maintenance personnel, contract workers, vendors, consultants (unless they are long-term, in which case guest access may be provided) and auditors.

Bonded Personnel: This is useful in cases where physical access to sensitive facilities is given to employees or outsiders such as contract employees. Bonding (contractors or employees being required to execute a financial bond) such personnel does not improve physical security but only reduces financial impact due to improper access/misuse of physical access.

Wireless Proximity Readers. A proximity reader does not require physical contact between the access card and the reader. The card reader senses the card in possession of a user in the general area (proximity) and enables faster access.

Alarm Systems/Motion detectors. Alarm systems provide detective controls and highlight security breaches to prohibited areas, access to areas beyond restricted hours, violation of direction of movement e.g. where entry only/exit only doors are used. Motion detectors are used to sense unusual movement within a predefined interior security area and thus detect physical breaches of perimeter security, and may sound a alarm.

Secured Distribution Carts: One of the issues in batch output control is to get the printed hardcopy reports (which may include confidential materials) securely across to the intended recipients. In such cases distribution trolleys with fixed containers secured by locks are used, the keys to the relevant container are held by the respective user team.

Cable locks: A cable lock consists of a plastic-covered steel cable that chains a PC, laptop or peripherals to the desk or other immovable objects.

Port controls: Port controls are devices that secure data ports (such as a floppy drive or a serial or parallel port) and prevent their use.

Switch controls: A switch control is a cover for the on/off switch, which prevents a user from switching off the file server's power.

Peripheral switch controls: These types of controls are lockable switches that prevent a keyboard from being used.

Biometric Mouse: The input to the system uses a specially designed mouse, which is usable only by pre-determined/pre-registered persons based on the fingerprint of the user.

Laptops Security: Securing laptops and portables represent a significant challenge, especially since, loss of laptops create loss of confidentiality, integrity and availability. Cable locks, biometric mice and encryption of the file system are some of the means available to protect laptops and their data.

Auditing Physical Access

Auditing physical access requires that the auditor to review the physical access risks and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

Risk Assessment

The auditor should satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures therefrom.

Controls Assessment

The auditor based on the risk profile evaluates whether physical access controls are in place and adequate to protect the IS assets against the risks.

Review of Documentation

Planning for review of Physical access controls requires examination of relevant documentation such as the Security policy and procedures, premises plans, building plans, Inventory list, cabling diagrams.

Testing of Controls

The auditor should review physical access controls for their effectiveness. This involves:

- ▶ Tour of organisational facilities including outsourced and offsite facilities.
- ▶ Physical inventory of computing equipment and supporting infrastructure.
- ▶ Interviewing personnel can also provide information on the awareness and knowledge of procedures.
- ▶ Observation of safeguards and physical access procedures. This would also inspection of:
 - ▼ Core computing facilities
 - ▼ Computer storage rooms
 - ▼ Communication closets
 - ▼ Backup and Off site facilities
 - ▼ Printer rooms
 - ▼ Disposal yards and bins
 - ▼ Inventory of supplies and consumables
- ▶ Some special considerations involve the following:
 - ▼ All points of entry/exit
 - ▼ Glass windows and walls
 - ▼ Moveable and modular cubicles
 - ▼ Ventilation/Air-conditioning ducts
 - ▼ False Ceiling and flooring panels.
- ▶ Review of Physical access procedures including user registration and authorization, authorization for special access, logging, review, supervision etc. Employee termination procedures should provide withdrawal of rights such as retrieval of physical devices such as smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organisation.
- ▶ Examination of physical access logs and reports. This includes examination of incident reporting logs, problem resolution reports.

Summary

The chapter deals with physical threats to information system assets. The first step in providing a secured physical environment for the information system assets is listing the various assets in the computing environment. These assets could range from hardware, software, facilities and people that form the computing environment. The next step is to identify the various threats and exposures the assets are exposed to. These threats could include unauthorized access to the resources, vandalism, public disclosure of confidential information and the like, The

main source of threats is from outside people and the employees of the organisation. However, the information assets are exposed to various other sources of threats like natural damage due environmental factors like flood, earthquake, fire and rain etc.

Various technical methods can be employed to secure the assets. These range from simple lock and bolts to very sophisticated biometric systems.

Auditing the physical security of the information assets involves risk assessment, evaluation of the controls and testing of controls through steps like tour of entire computing environment, actual examination of the security features, interview of the relevant personnel and examination of the documentation.



7 Environmental Access Controls

✂ Learning Goals ✂

To understand:

- ▶ Environmental Issues and Exposures
- ▶ Administrative and Technical Controls for the Computing Environment
- ▶ Audit and evaluation of Environmental Controls

Introduction

This section examines the risks to IS resources arising from undesired changes in the environment. Environmental threats to information assets include threats primarily relating to facilities and supporting infrastructure, which house and support the computing equipment, media and people. IS Auditor should review all factors that adversely bear on the confidentiality, integrity and availability of the information, due to undesired changes in the environment or ineffective environmental controls.

IS Assets: Objects of Environmental Controls

The objects to be protected in environmental are much the same as discussed in the section on physical access controls. However from the perspective of environmental exposures and controls, information systems resources may be categorized as follows, with the focus primarily on facilities which house:

1. Hardware and Media: Includes Computing Equipment, Communication equipment, and Storage Media
2. Information Systems Supporting Infrastructure or Facilities: This typically includes the following:
 - ▼ Physical Premises, like Computer Rooms, Cabins, Server Rooms/Farms, Data Centre premises, Printer Rooms, Remote facilities and Storage Areas
 - ▼ Communication Closets
 - ▼ Cabling ducts
 - ▼ Power Source
 - ▼ Heating, Ventilation and Air Conditioning (HVAC)
3. Documentation
4. Supplies
5. People

Environmental Threats and Exposures

Undesired unintentional or intentional alteration in the environment in which computing resources function can result in threats to availability of information systems and integrity of information. Exposures from environmental threats include total or partial loss of computing facilities, equipment, documentation and supplies causing loss or damage to organisational data and information and more importantly people. The threats can be broadly classified as Natural and Man-made.

Natural

Threats to facilities and environment from natural causes can significantly and adversely impact the availability, integrity and confidentiality of information. Examples include:

- ▶ Natural disasters such as earthquakes, floods, volcanoes, hurricanes and tornadoes
- ▶ Extreme variations in temperature such as heat or cold, snow, sunlight, etc.
- ▶ Static electricity
- ▶ Humidity, vapours, smoke and suspended particles
- ▶ Insects and organisms such as rodents, termites and fungi
- ▶ Structural damages due to disasters

Man-made

Human induced threats again can be unintentional or intentional, examples of which are:

- ▶ Fire due to negligence and human action
- ▶ War Action and Bomb threats
- ▶ Power – uncontrolled/unconditioned power, spikes, surges, low voltage
- ▶ Equipment failure
- ▶ Failure of Air-conditioning, Humidifiers, Heaters
- ▶ Food particles and residues, undesired activities in computer facilities such as smoking.
- ▶ Structural damages due to human action/inaction and negligence
- ▶ Electrical and Electromagnetic Interference (EMI) from Generators, motors.
- ▶ Radiation
- ▶ Chemical/liquid spills or gas leaks due to human carelessness or negligence

Some examples of exposures from violation of environmental controls:

- ▶ A fire could destroy valuable computer equipment and supporting infrastructure and invaluable organisational data. Usually the use/storage of thermocole or Styrofoam (technically called Expanded Polystyrene) material, inflammable material used for construction

of the server cabin, false ceiling aggravate the probability of fire and loss due to fire.

- ▶ Magnetic tapes uses materials which are inflammable.
- ▶ Poor quality of power cables can over-heat and cause fire.
- ▶ Lightening may burn up communication devices and computing equipment due to improper earthing or grounding.
- ▶ Continuous process systems bear the risk of internal component damage due to improper air conditioning or high humidity.
- ▶ Damage of keyboards and other computing devices due to accidental dropping of beverages, liquid, etc.
- ▶ Food particles leftover in computer facilities attract rodents, insects which can damage cabling, hard disks.
- ▶ Chemical or liquid spills from a nearby unit may seep into the IPF (Information Processing Facility) thereby damaging equipment.
- ▶ Sudden surges in power or other voltage fluctuations can irreversibly damage computer equipment.
- ▶ Fungi formation on tapes can leads to tapes and disks being not readable.
- ▶ EMI (Electromagnetic Interference) from generators can damage integrity of contents on magnetic media.
- ▶ Water leakages can induce shocks and short circuits.

Techniques of Environmental Control

The IS supporting infrastructure and facilities not only provide the conducive environment for the effective and efficient functioning of the IPF but should also protects the contents of such facilities from undesirable variations in the environment.

Based on the risk profile, computing equipment, supporting equipment, supplies, documentation and facilities should be appropriately situated, protected to reduce risks from environmental threats and hazards. These controls are broadly classified into Administrative and Technical controls.

Administrative Controls

Choosing and designing a safe site

The considerations during choosing a location for the facility are (as discussed in the section on Physical Access Controls):

- ▶ **Visibility.** Facilities such as data centres should not be visible or identifiable from the outside, that is, no windows or directional signs.
- ▶ **Local considerations.** What is the local rate of crime (such as forced entry and burglary)?
- ▶ **Natural disasters.** Probability of natural disasters as compared to other locations? Natural disasters can include weather-related problems (wind, snow, flooding, and so forth) and earthquake faults.

Module 3, Chapter 7

- ▶ **Transportation.** Does the site have a problem due to excessive air, highway, or road traffic?
- ▶ **External services.** The relative proximity of the local emergency services, such as police, fire, and hospitals or medical facilities has to be factored in while choosing a site.

Considerations during designing a site are as follows:

- ▶ **Walls:** Entire walls, from the floor to the ceiling, must have an acceptable fire rating. Closets or rooms that store media must have a high fire rating.
- ▶ **Ceilings:** Issues of concern regarding ceilings are the weight-bearing rating and the fire rating.
- ▶ **Floors:** If the floor is a concrete slab, the concerns are the physical weight it can bear and its fire rating. If it is a raised flooring the fire rating, its electrical conductivity (grounding against static build-up), and that it employs a non-conducting surface material are major concerns. Electrical cables must be enclosed in metal conduit, and data cables must be enclosed in raceways, with all abandoned cable removed. Openings in the raised floor must be smooth and nonabrasive, and they should be protected to minimize the entrance of debris or other combustibles. Ideally, an IPF should be located between floors and not at or near the ground floor, nor should it be located at or near the top floor.
- ▶ **Windows:** Windows are normally not acceptable in the data centre. If they do exist, however, they must be translucent and shatterproof.
- ▶ **Doors:** Doors in the computer centre must resist forcible entry and have a fire rating equal to the walls. Emergency exits must be clearly marked and monitored or alarmed. Electric door locks on emergency exits should revert to a disabled state if power outages occur to enable safe evacuation. While this may be considered a security issue, personnel safety always takes precedence, and these doors should be manned in an emergency.
- ▶ **Media Protection:** Location of media libraries, fire proof cabinets, kind of media used (fungi resistant, heat resistant).
- ▶ **Sprinkler system and fire resistance:** The fire-resistance rating of construction material is a major factor in determining the fire safety of a computer operations room. Generally, the computer room must be separated from other occupancy areas by construction with a fire-resistant rating of not less than two hours.
- ▶ **Water or gas lines:** Water drains should be “positive,” that is, they should flow outward, away from the building, so they do not carry contaminants into the facility.
- ▶ **Air conditioning:** AC units should have dedicated power circuits. Similar to water drains, the AC system should provide outward, pos-

itive air pressure and have protected intake vents to prevent air-carried toxins from entering the facility.

- ▶ **Electrical requirements:** The facility should have established backup and alternate power sources.

Other Administrative and Maintenance Controls

1. Physical and environmental security should form a critical component of the security policy.
2. As part of facilities planning, the security policy should provide for specific procedures for analysis and approval of facilities building and refurbishment plan. Depending on the size and nature of computing facilities, a separate function should exist for facilities planning and management. The following aspects need to be considered in this context:
 - ▼ As part of environmental security clearance, procedures should be prescribed to ensure that all aspects relating to facilities planning are adequately considered.
 - ▼ Approved list of materials to be used for construction of facilities, based on the class of computing facilities, the specification of equipment to be housed in such facilities should need consideration.
 - ▼ The organisation chart should provide for designated personnel assigned with the responsibility of risk assessment procedures as a dynamic function. The risk profile of the organisation should take into consideration newer environmental threats. A few examples of threats to be considered are given below:
 - ▲ Installation of a generator by a neighbour.
 - ▲ Sudden changes in climate leading to extreme changes in humidity levels.
 - ▲ Building construction in the vicinity of IPF leading to increase in suspended dust particles in the environment.
 - ▲ Raising of foundation and flooring by a neighbour causing change in the flow of rainwater.
 - ▲ Installation of high power consumption equipment adversely affecting the quality of power.
3. Documentation of physical and geographical location and arrangement of computing facilities and environmental security procedures should be modified promptly for any changes thereto. Access to such documentation should be strictly controlled. For example, knowledge of location and scheme of ventilation ducts can be used by a perpetrator to gain unauthorized entry to sensitive facilities which otherwise may be secured by physical and logical controls.
4. Responsibility and accountability for environmental controls planning and management should be fixed and should be expressly communicated as part of job description.

Module 3, Chapter 7

5. Awareness and training initiatives should encompass educating employees and stakeholders on environmental exposures and controls and their responsibilities thereof. New employee induction programs should include informing and educating employees on environmental control procedures, prohibited activities (eating, smoking, drinking inside IPF), and maintaining secrecy and confidentiality. Care should also be taken to ensure that sharing such information should not result in risks, where unauthorized persons could gain knowledge of sensitive environmental control vulnerabilities.
6. Disasters result in increased environmental threats e.g. smoke from a fire in the neighbourhood or in some other facility of the organisation would require appropriate control action, evacuation plan should be in place and evacuation paths should be prominently displayed at strategic places in the organisation.
7. Reporting procedures should be in place to enable and support reporting of any environmental threats to a specified controlling authority.
8. Periodic inspection, testing and supervision of environmental controls should form a part of the administrative procedures. The tests of such inspection, tests and drills should be escalated to appropriate levels in the organisation.
9. In most cases installation and maintenance of environmental controls involves the services of third parties such as air conditioning, fire safety equipment, civil contractors, carpenters. By virtue of their scope of work, knowledge of and access to sensitive computing facilities and environmental control vulnerabilities are available to such agencies. Procedures should include detailed analysis of considerations such as, whether to outsource, choice of such agency, background verification, security bonding, controlled access of maintenance staff and performance appraisal.
10. A comprehensive maintenance and inspection plan is critical to the success of environmental security and controls. Preventive maintenance plan and management procedures should be in place. This is a critical aspect of environmental control procedures, negligence in respect of which can lead to exposing the IPF to risks, e.g. prolonged ineffectiveness/failure of air conditioning facility can lead to risks of damage to servers and thereby loss of organisational data; a fire extinguisher not working at time of disaster due to negligence in refilling and maintenance. Maintenance plans should also include evaluation of effectiveness and efficiency of environmental facilities such as electric power distribution, heating plants, water, sewage, and other utilities required for system operation or staff comfort.
11. Failure modes of each utility, risks of utility failure, should be identified, parameterized and documented. This includes estimating the MTBF (Mean Time Between Failures) and MTTR (Mean Time To

Repair). Planning for Environmental controls would need to evaluate alternatives with low MTBF or installing redundant units. Stocking spare parts on site and training maintenance personnel can reduce MTTR. Each of these strategies can be evaluated by comparing the reduction in risk with the cost to achieve it.

12. Environmental controls should be documented and a suitable preventive maintenance should be put in place administered through schedules and logs.
13. Documented and tested emergency evacuation plans should consider the physical outlay of the premises and orderly evacuation of people, shut down of power and computer equipment, activation of fire suppression systems.
14. Administrative procedures should also provide for Incident Handling procedures and protocols due to environmental exposures.

Technical Controls

Some of the techniques for implementing control to protect against environmental risks are:

Fire-resistant Walls, Floors and Ceilings: The construction of IPF should use fire-resistant materials for walls, floors and ceilings. Depending on application and investment, manufacturers offer materials with varied fire ratings. Fire rating resistance of at least 2 hours is generally recommended.

Concealed Protective Wiring: Power and Communication cables should be laid in separate fire resistant panels and ducts. The quality rating of power cables should match the load and manufacturers specifications.

Ventilation and Air Conditioning: The temperature in the IPF should be controlled depending on the type of equipments and processing. Improper maintenance of temperature leads to overheating of internal components. It should be examined if uninterruptible power supply systems should supply power HVAC equipment that support critical IPF units.

Power Supplies: Computing equipment can be subject to risks of power failure and other power anomalies. Power supply should conform to computing equipment manufacturer specifications. Many elements can threaten power systems, the most common being noise and voltage fluctuations. Noise in power systems refers to the presence of electrical radiation in the system that is unintentional and interferes with the transmission of clean power. There are several types of noise, the most common being electromagnetic interference (EMI) and radio frequency interference (RFI). Voltage fluctuations are classified as Sag (momentary low voltage), Brownout (prolonged low voltage), Spike (momentary high voltage), Surge (prolonged high voltage) and Blackouts (complete loss of power).

Module 3, Chapter 7

Some of the controls to ensure uninterrupted delivery of clean power are:

- ▶ **Uninterruptible Power Supply(UPS)/ Generator:** UPS usually consist of battery backup or kerosene powered generator that interfaces with the external power supplied to the equipment. On interruption in external power supply, the control is immediately switched to the battery back-up. Depending on the application, UPS are available with battery backup of a few minutes to a number of days. UPS can be on-line or off-line. UPS generally is a good solution in case of applications enabling their proper closure of processing and systems. In respect of continuous process equipments, UPS may fail to meet the purpose if regular power supply is not available for an prolonged period of time. Diesel or kerosene generators could also be used, but they require some time to be switched on and the power from generators has to be cleansed before delivery to computer systems.
- ▶ **Electrical Surge Protectors/Line Conditioners:** Power supply from external sources such a grid and generators are subject to many quality problems such as spikes, surges, sag and brown outs, noise, etc. Surge protectors, spike busters and line conditioners are equipment which cleanse the incoming power supply of such quality problems and delivery clean power fit for the equipment.
- ▶ **Power leads from two sub-stations:** Failure of continued power supply to some high consumption continuous processing could even result in concerns regarding public safety such as refineries, nuclear reactors and hospitals. Electric power lines may be exposed to many environmental and physical threats such as floods, fire, lightning, careless digging, etc. To protect against such exposures, redundant power lines from a different grid supply should be provided for. Interruption of one power supply should result in the system immediately switching over to the stand-by line.

Smoke Detectors and Fire Detectors: Smoke and fire detectors activate audible alarms or fire suppression systems on sensing a particular degree of smoke or fire. Such detectors should be placed at appropriate places, above and below the false ceiling, in ventilation and cabling ducts. In case of critical facilities, such devices must be linked to a monitoring station (such as fire station). Smoke detector should supplement and not replace fire suppression systems.

Fire Alarms: Manually activated fire alarms switches should be located at appropriate locations prominently visible and easily accessible in case of fire (but should not be easily capable of misuse during other times). By manual operation of switch or levers, these devices activate an audible alarm and may be linked to monitoring stations both within and/or outside the organisation.

Emergency Power Off: When there arises a necessity of immediate power shutdown during situations such as computer facility fire or emergency evacuation, emergency power-off switches should be provided. There should be one within the computer facility and another just outside the computer facility. Such switches should be easily accessible and should be shielded to prevent accidental use.

Water detectors: Risks to IPF equipment from flooding and water logging can be controlled by use of water detectors placed under false flooring or near drain hole. Water detectors should be placed on all unattended or unmanned facilities. Water detectors on detecting water activate an audible alarm.

Centralised Disaster monitoring and control Systems: Such systems provide for an organisation-wide network control wherein all detection devices, alarms and corrective/suppression devices are controlled from a central monitoring command and control. It is necessary that such systems are powered by a more secure and reliable/uninterrupted power supply. Such systems should be failure tolerant and involve low maintenance.

Fire Suppression Systems

Combustibles are rated as either Class A, B, or C based upon their material composition, thus determining which type of extinguishing system or agent is used. Fires caused by common combustibles (like wood, cloth, paper, rubber, most plastics) are classed as Class A and are suppressed by water or soda acid (or sodium bicarbonate). Fires caused by flammable liquids and gases are classed as Class B and are suppressed by Carbon Dioxide (CO₂), soda acid, or Halon. Electrical fires are classified as Class C fires and are suppressed by Carbon Dioxide (CO₂), or Halon. Fire caused by flammable chemicals and metals (such as magnesium and sodium) are classed as Class D and are suppressed by Dry Powder (a special smothering and coating agent). Class D fires usually occur only in places like chemical laboratories and rarely in office environments. **NOTE THAT USING THE WRONG TYPE OF EXTINGUISHER WHILE SUPPRESSING A FIRE CAN BE LIFE-THREATENING.**

Broadly, Fire Suppression systems for facilities are classed into (a) Water based systems and (b) Gas based systems

Water Based Systems

- ▶ **Wet Pipe Sprinklers:** In this case, sprinklers are provided for at various places in the ceiling or on the walls and water is charged in the pipes. As generally implemented a fusible link in the nozzle melts in the event of a heat rise, causing a valve to open and allowing water to flow.

Module 3, Chapter 7

These are considered the most reliable but however they suffer from the disadvantage of leakage, breakage of pipes exposing the IPF to the risks of dampness and equipments suffering water damage.

- ▶ **Dry-Pipe Sprinklers:** These are similar to the wet pipe sprinklers except that in this the water is not kept charged in pipes but pipes remain dry and upon detection of heat rise by a sensor, water is pumped into the pipes. This overcomes the disadvantage with wet pipe systems of water leakages etc.
- ▶ **Preaction:** At the present time, this is the most recommended water-based fire suppression system for a computer room. It combines both the dry and wet pipe systems by first releasing the water into the pipes when heat is detected (dry pipe) and then releasing the water flow when the link in the nozzle melts (wet pipe). This feature enables manual intervention before a full discharge of water on the equipment occurs.

Gas Based Systems

- ▶ **Carbon-dioxide:** Such systems discharge CO₂ thus effectively cutting of oxygen supply from the air, which is a critical component for combustion. However, CO₂ being potentially lethal for human life, such systems are recommended only in unmanned computer facilities or in portable or hand-held fire extinguishers. Portable fire extinguishers commonly contain CO₂ or soda acid and should be:
 - ▼ Commonly located at exits
 - ▼ Clearly marked with their fire types
 - ▼ Checked regularly by licensed personnel
- ▶ **Halon:** Halon was once considered the most suitable agent for fire suppression. Halon is an inert gas, does not damage equipments as water systems do and does not leave any liquid or solid residues. However, Halon is not considered safe for humans beyond certain levels of concentration and is an ozone-depleting agent and hence environmentally unfriendly. Under an international agreement, the Montreal Protocol, the production of Halon has been suspended from 1994.

Integration and Fine Tuning of Environmental Controls

As part of environmental risk assessment, facilities planning and facilities management, it is critical to consider the overall effectiveness, efficiency of controls. Planning for Environmental Controls should consider interdependencies in respect of nature of IS assets being secured, vulnerabilities in respect of such assets and nature of other controls such as logical and physical controls. The Security Policy should orchestrate the overall design, effectiveness and efficiency of controls to ensure

that investment in environmental controls are optimum without compromise on security.

Audit and Evaluation of Environmental Controls

Audit of environmental controls should form a critical part of every IS audit plan. The IS Auditor should satisfy himself or herself not only as regards the effectiveness of various technical controls but importantly assure himself or herself that the overall controls assure safeguarding the business against environmental risks. Some of the critical audit considerations that an IS Auditor should take into account while conducting his audit are given below:

Audit Planning and Assessment

- ▶ As part of Risk assessment, the risk profile should include all kinds of environmental risks that the organisation is exposed to, which should include taking stock of both natural and man-made threats. The profile should be periodically reviewed to ensure updating the profile with new risks that may have arisen.
- ▶ The Controls assessment should include examining that controls are in place to safeguard the organisation against all acceptable risks and should include newer risks.
- ▶ The Security Policy of the organisation should be reviewed to assess policies and procedures on safeguarding the organisation against environmental risks are adequately covered.
- ▶ The building plans, wiring plans, surroundings, power and cable wiring etc. should be reviewed to determine appropriateness of location of IPF.
- ▶ The IS auditor should interview relevant personnel to satisfy himself regarding employee awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, evacuation procedures, to assess if adequate incident reporting procedures exist.
- ▶ Review administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures.

Audit of technical controls

As part of audit procedures, the audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices, which may include the following activities:

- ▶ Inspect the IPF and examine the construction with regard to the type of materials used for construction by referring to the appropriate documentation.

Module 3, Chapter 7

- ▶ Visually examine the presence of water and smoke detectors, examine power supply arrangements to such devices, testing logs, etc.
- ▶ Examine location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers and ensure their adequate and appropriate.
- ▶ Examine emergency procedures, evacuation plan and marking of fire exits. If considered necessary, the IS Auditor can also require a mock drill to test the preparedness with respect to disaster.
- ▶ Examine documents for compliance with legal and regulatory requirements as regards fire safety equipment, external inspection certificate, shortcomings pointed out by other inspectors/auditors.
- ▶ Examine power sources and conduct tests to assure quality of power, effectiveness of power conditioning equipment, generators, simulate power supply interruptions to test effectiveness of back-up power.
- ▶ Examine environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- ▶ Examine complaint logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- ▶ Observe activities in the IPF for any undesired activities such as smoking, consumption of eatables etc.

Documentation of findings

As part of the audit procedures, the IS auditor should also document all findings as part of working papers. The working papers could include audit assessment, audit plan, audit procedure, questionnaires, interview sheets, inspection charts, etc.

Summary

The focus of the chapter is on environment based threats to information system assets. The first step in providing a secure physical environment for the information system assets is listing down the various assets in the computing environment. These assets could range from hardware, software, facilities and people that form the computing environment. The next step is to identify the plausible threats and exposures the assets could be exposed to. The main source of threats considered here are environmental and natural threats. Information assets are exposed to various other sources of threats like natural damage due environmental calamities like floods, earthquakes, fires, rains etc. Various technical and administrative methods can be employed to secure the assets.

Auditing the physical security of the information assets involves risk assessment, evaluation of the controls and testing of controls through touring the entire computing environment, actually examining the se-

curity features and documentation as well as interviewing relevant personnel



Questions

- Q1. A requirement that information and programs are changed only in a specified and authorized manner is called:
- A. Confidentiality
 - B. Availability
 - C. System integrity
 - D. Data integrity
- Q2. A requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system is called
- A. Confidentiality
 - B. Availability
 - C. System integrity
 - D. Data integrity
- Q3. A requirement intended to assure that systems work promptly and service is not denied to authorized users is called:
- A. Confidentiality
 - B. Availability
 - C. System integrity
 - D. Data integrity
- Q4. A requirement that private or confidential information should not be disclosed to unauthorized individuals is called:
- A. Confidentiality
 - B. Availability
 - C. System integrity
 - D. Data integrity
- Q5. Who has the authority to delegate the operational responsibility of an organisation's data?
- A. Data user
 - B. Senior manager
 - C. Data custodian
 - D. Data owner
- Q6. As it applies to security, which selection best defines the difference between the role of an Information Owner and the role of an Information Custodian?
- A. The Information Custodian applies the data classification scheme and protection mechanisms after the initial assign-

Module 3, Questions

- ment by the Chief Information Officer.
 - B. The Information Owner is a managing partner of the organization and the Information Custodian is an hourly employee.
 - C. The Information Custodian applies the data classification scheme and protection mechanisms after the initial assignment by the Owner.
 - D. The Information Owner applies the data classification scheme and protection mechanisms after the initial assignment by the Custodian.
- Q7. In which of the following access control model is it necessary to for each resource to be classified and for each user be assigned a clearance level.
- A. Supervisory access control
 - B. Mandatory access control
 - C. Discretionary access control
 - D. Reactionary access control
- Q8. Commercial organisations are more likely to use
- A. Discretionary access control.
 - B. Unrestricted access control.
 - C. Mandatory access control.
 - D. Compulsory access control.
- Q9. Military and defence organisations are more likely to use
- A. Discretionary access control.
 - B. Unrestricted access control.
 - C. Compulsory access control.
 - D. Mandatory access control.
- Q10. A principle that advocates for minimal user profile privileges on computers, based on users' job necessities is called:
- A. Principle of maximum privilege.
 - B. Principle of zero privilege.
 - C. Principle of least privilege.
 - D. Mandatory access control.
- Q11. The first step in any security administration is:
- A. Implement good access control mechanisms.
 - B. Ensure that good backup procedures have been set up.
 - C. Ensure that each user has a separate login.
 - D. Develop a good security policy for the organisation.
- Q12. When drafting an information security policy, why would it be important to require that the use of communications test equipment be controlled?
- A. The equipment may damage network hardware.
 - B. The equipment is complicated and the user needs specific

Module 3, Questions

- training to use it correctly.
- C. The equipment can be used to view information passing through the network.
 - D. The equipment is expensive and needs to be protected from theft.
- Q13. Which of the following need NOT be considered before hosting a new online privacy policy?
- A. Business practices
 - B. Business partners
 - C. Proposed users
 - D. Nature of the site
- Q14. Which of the following should NOT be included in an Organisation's information security policy?
- A. Identity of sensitive security features
 - B. Access philosophy
 - C. Access authorisation
 - D. Importance of security awareness
- Q15. While conducting an audit, the auditor should
- A. Insist that a security policy exists.
 - B. Not insist for a security policy.
 - C. Insist that a security policy exists, and accept the existing policy.
 - D. Insist that a security policy exists. However he may not accept the existing policy.
- Q16. To enforce the email policy, the management need NOT:
- A. Educate employees
 - B. Take prompt action in case of misuse or complaints
 - C. Educate third parties
 - D. Prohibit subscription to e-newspapers and e-groups
- Q17. The greatest risk of inadequate definition of policy relating to ownership of data and systems is:
- A. All users are authorised to originate, modify and delete data.
 - B. Accountability cannot be established.
 - C. Difficulty in coordinate change within large organisations.
 - D. Audit recommendations may not be established.
- Q18. A general guideline of a security policy does NOT
- A. Keep the policy a secret
 - B. Identify acceptable activities
 - C. Update the policy
 - D. Identify and determine what is to be protected.
- Q19. A detailed policy on firewalls should NOT:
- A. Ensure that the firewall is logically secured

Module 3, Questions

- B. Include guidelines for assessment of logs
 - C. Ensure that the firewall is physically secured
 - D. Include log reports
- Q20. While evaluating the IT control environment for obtaining an understanding of the management's control over IT activities, the auditor should consider:
- A. The functions of the IT steering committee
 - B. The IT strategy of the management
 - C. The Security policy
 - D. The user's perception of IT
- Q21. If a thief steals an ATM card and tries to break the PIN number by trying all combinations, what type of attack will it be classified as?
- A. Keystroke logging
 - B. Man in the middle
 - C. Biometric
 - D. Bruteforce
- Q22. Which of the following is the best example of three-factor authentication?
- A. An ATM card and a PIN.
 - B. A thumbprint and password.
 - C. A smart card, password and thumbprint.
 - D. A RADIUS server.
- Q23. A software programmer writes a program to review the payroll records each month to ensure that he is still employed. If the programmer's name is removed from the payroll, the program will activate another piece of code to destroy vital files on the organization's system. Which of the following terms will describe this type of malicious code?
- A. ActiveX
 - B. Logic Bomb
 - C. Virus
 - D. Denial of Service
- Q24. Which term often means a piece of code left behind in the system that will allow the original programmer back into the system?
- A. Trap Door
 - B. Flap Jack
 - C. Unicode
 - D. Stealth Code
- Q25. Which of the following would NOT protect a system from computer viruses?
- A. Write protect all diskettes once they have been virus checked
 - B. Scan any new software before it is installed

Module 3, Questions

- C. Do not allow vendors to run demonstration on company owned machines
 - D. Boot only from diskettes that were initially checked for viruses
- Q26. Passwords are used as a basic mechanism to identify and authenticate a system user. Which of the following password-related factors cannot be tested by an IS auditor?
- A. Password length
 - B. Password lifetime
 - C. Password secrecy
 - D. Password storage
- Q27. Which of the following types of database access control is the most difficult to enforce?
- A. Name-dependent access control
 - B. History-dependent access control
 - C. Content-dependent access control
 - D. Context-dependent access control
- Q28. Viruses that can change their appearance are known as:
- A. Polymorphic virus
 - B. Boot sector virus
 - C. Stealth virus
 - D. Macro virus.
- Q29. “Biometric authentication” is based on:
- A. Design features
 - B. Logical features
 - C. Depends upon the application to be authenticated
 - D. Physical features
- Q30. Which of the following feature may seriously affect or nullify the utility of audit trails?
- A. Passwords are not recorded in the audit trail.
 - B. Security administrator cannot amend the details in the audit trail.
 - C. Audit trail records can be amended by the users.
 - D. Date and time stamps are recorded automatically.
- Q31. Identify the correct statement with respect to guidelines for data-entry screens?
- A. Both bright colours and automatic tabbing are to be avoided.
 - B. Both bright colours and automatic tabbing should be used as often as possible.
 - C. Bright colours should be avoided and automatic tabbing should be used as often as possible.
 - D. Bright colours should be used as often as possible while automatic tabbing should be avoided.

Module 3, Questions

- Q32. Data entry screens should have:
- A. a slow but consistent display rate.
 - B. a fast and consistent display rate.
 - C. a slow and varying display rate
 - D. a slow and varying display rate
- Q33. Which of the following checks can significantly reduce transcription errors?
- A. Range checks
 - B. Limit checks
 - C. Check digits
 - D. Size checks
- Q44. If the product number A5723 is coded as A5753, this is an example of a:
- A. Truncation error
 - B. Double transposition error
 - C. Random error
 - D. Transcription error
- Q35. Which of the following is not a validation done on instruction input?
- A. Holistic validation
 - B. Lexical validation
 - C. Semantic validation
 - D. Syntactic validation
- Q36. Which of the following is a control problem associated with spooling software?
- A. It is error-prone because the software is highly complex.
 - B. It can be used to obtain an unauthorized copy of a report.
 - C. The output could be redirected to another printer.
 - D. The output could be cancelled before printing.
- Q37. A company's labour distribution report requires extensive corrections each month because of labour hours charged to inactive jobs. Which of the following data processing input controls appears to be missing?
- A. Completeness test
 - B. Limit check
 - C. Validity test
 - D. Control total
- Q38. A check to ensure that the same data is not keyed twice is called:
- A. Sequence checks
 - B. Limit check
 - C. Missing data check
 - D. Duplicate check

Module 3, Questions

- Q39. As a quality assurance measure in the batch processing of accounts payable data, a firm sums the account numbers for all accounts processed. This procedure results in a:
- A. Hash total
 - B. Batch number
 - C. Parity check
 - D. Check sum
- Q40. The purpose of a file retention date is to:
- A. Enable files with the same generation number to be distinguished
 - B. Prevent the file from being overwritten before the expiry of the retention date
 - C. Indicate when the file should be recovered from production activities
 - D. Prevent the file from being read before expiry of the retention date
- Q41. A firewall is a system for
- A. Enforcing an access control policy
 - B. Preventing viruses
 - C. Preventing intruders
 - D. Assisting auditors.
- Q42. Cryptographic systems provide for:
- A. Linearity of messages.
 - B. Integrity of messages.
 - C. Intelligibility of messages.
 - D. Availability of messages.
- Q43. Which of the following terms describes a form of dial-up access control whereby the user dials the desired phone number, authenticates with the server, hangs up, and then the server dials the client, establishing the connection?
- A. Dial Back
 - B. Redialing
 - C. Call Waiting
 - D. Call Forwarding
- Q44. Which technique is best described as method of providing information for error detection, usually calculated by summing a set of values by both the sender of the information and the receiver of the transmission?
- A. Uuencode
 - B. Algorithm
 - C. Data Mining
 - D. Checksum

Module 3, Questions

- Q45. If the series of data bits, 11001011, is received as 11001000 then it is called a:
- A. Single bit error
 - B. Multiple-bit error
 - C. Burst error
 - D. Parity error.
- Q46. Which of the following provides error detection and error correction?
- A. Cyclic Redundancy Check
 - B. Checksum
 - C. Parity check
 - D. Hamming code
- Q47. The integrity of system cannot be lost due to
- A. Trojan Horse
 - B. Packet Sniffers
 - C. Brute force attack
 - D. Firewalls
- Q48. A cookie gets data from:
- A. Whatever the user enters from the console on a web page.
 - B. What the web server sends to the web browser.
 - C. User application programs.
 - D. The operating system and the web browser used at the client-end.
- Q49. A message authentication code is used to protect against:
- A. Changes to the content of a message.
 - B. Traffic analysis.
 - C. Release of message contents.
 - D. Exposures that arise when PINs are transmitted in the clear.
- Q50. A firewall cannot:
- A. Protect against unauthorized logins from external networks.
 - B. Protect the network against users connecting to the Internet by dialling to their ISP using their office telephone and a modem.
 - C. Appear transparent to their users.
 - D. Log traffic to and from the local network.
- Q51. Which of the following physical control would be most appropriate in a high security environment?
- A. Combination locks
 - B. Identification badges
 - C. Electronic Door Locks
 - D. Biometric Door Locks

Module 3, Questions

- Q52. To prevent the unauthorized use of floppy drives, which of the following controls is suitable?
- A. Switch controls
 - B. Cable locks
 - C. Port controls
 - D. Biometric mouse
- Q53. For physical and environmental security, in which of the following areas should policies and procedures be framed?
- A. Independent (third-party) assurances
 - B. Layout of facilities
 - C. System Development Life Cycle (SDLC)
 - D. None of the above
- Q54. The risk of piggybacking, in which an unauthorized person could enter the secured facility by closely following an authorized person, may be controlled by:
- A. Deadman Doors
 - B. Bolting door locks
 - C. Electronic Door Locks
 - D. Cipher locks
- Q55. Which of the following may be used to protect a laptop?
- A. Wireless Proximity Readers
 - B. Switch controls
 - C. Port controls
 - D. Biometric mice
- Q56. Which of the following would be used to deter casual intruders?
- A. Biometric locks
 - B. Port controls
 - C. Perimeter fencing
 - D. Wireless Proximity Readers
- Q57. As a security precaution, visitors are escorted by a pre-designated responsible employee or security staff. Which of the following would be classified as visitors?
- A. Vendors only.
 - B. Vendors and maintenance personnel only.
 - C. Vendors, maintenance personnel and contract workers only.
 - D. Vendors, maintenance personnel, contract workers and auditors.
- Q58. The purpose of employee bonding is to:
- A. Reduce financial impact due to improper access/misuse of physical access
 - B. Prevent fraud.
 - C. Encourage employees to report access violations

Module 3, Questions

- D. Improve physical security.
- Q59. Access time is quickest with of the following devices?
 - A. Bolting door locks
 - B. Electronic Door Locks
 - C. Combination door locks
 - D. Wireless Proximity Readers
- Q60. A device to detect breaches of physical security is:
 - A. Switch controls
 - B. Deadman Doors
 - C. Motion detectors
 - D. Identification badges
- Q61. A 'Dry pipe', which is an arrangement to extinguish fires is:
 - A. A Sprinkler system where the water is in the pipe, but the outside of the pipe is dry.
 - B. A Halon gas system that contains a dry pipe.
 - C. A carbon dioxide (CO₂) gas system that has a dry chemical to extinguish a fire.
 - D. A sprinkler system where the water is not kept charged in pipes but pipes remain dry and upon detection of heat rise by a sensor, water is pumped into the pipes.
- Q62. While auditing the environment controls the auditor should confirm that:
 - A. LAN file server facility has dust, smoke and other particulate matters
 - B. Consumption of food, beverage and tobacco is allowed
 - C. Fire protection equipment are adequate and appropriate
 - D. Air conditioning, humidity control system are followed as desired by the users of the LAN
- Q63. Surge, spike and sag are types of
 - A. Biometric systems
 - B. Electrical fluctuations
 - C. Fire suppression systems
 - D. Electromagnetic radiations
- Q64. Which of the following is NOT an environmental control?
 - A. Biometric devices
 - B. Line conditioners
 - C. Air conditioners
 - D. Fire suppression systems
- Q65. Which of the following is the most recommended water-based fire suppression system for a computer facility?
 - A. Dry pipe system
 - B. Wet pipe system

- C. Drip pipe system
D. Preaction system
- Q66. Which of the following gas-based fire suppression system would you find in an unmanned computer facility?
A. Argon
B. Halon
C. Carbon-dioxide
D. Oxygen
- Q67. How many emergency power-off switches should provided in a computer facility?
A. One
B. Two
C. Three
D. Four
- Q68. In an ideally equipped data centre, the wall, ceiling, etc should be made of fire resistant materials. For how long is it recommended that they should resist a fire?
A. 2 Hours
B. 1 Hour
C. 30 Minutes
D. 3 Minutes
- Q69. Identify the correct statement.
A. There should be no water drains near a computing facility.
B. Water drains should be “negative”, that is, they should flow inward, toward the building.
C. Water drains can be either “positive” or “negative”.
D. Water drains should be “positive”, that is, they should flow outward, away from the building.
- Q70. Identify the correct statement.
A. Fire suppression systems make smoke detectors redundant.
B. Smoke detectors make fire suppression systems redundant.
C. Smoke detector should supplement fire suppression systems.
D. Neither smoke detector nor supplement fire suppression are necessary.

Answers

QUESTION No	1	2	3	4	5	6	7	8	9	10
ANSWERS	D	C	B	A	D	C	B	A	D	C

QUESTION No	11	12	13	14	15	16	17	18	19	20
ANSWERS	D	C	B	A	D	C	B	A	D	C

Module 3, Questions

QUESTION No	21	22	23	24	25	26	27	28	29	30
ANSWERS	D	C	B	A	D	C	B	A	D	C

QUESTION No	31	32	33	34	35	36	37	38	39	40
ANSWERS	A	B	C	D	A	B	C	D	A	B

QUESTION No	41	42	43	44	45	46	47	48	49	50
ANSWERS	A	B	A	D	C	D	D	B	A	B

QUESTION No	51	52	53	54	55	56	57	58	59	60
ANSWERS	D	C	B	A	D	C	D	A	D	C

QUESTION No	61	62	63	64	65	66	67	68	69	70
ANSWERS	D	C	B	A	D	C	B	A	D	C

References

- ▶ Information Security Management Handbook, Fourth Edition, Volume I, by Micki Krause (Editor), Harold F. Tipton (Editor) (Hardcover)
- ▶ The Process of Network Security by Thomas A. Wadlow (Paperback)
- ▶ Mastering Network Security by Chris Brenton
- ▶ Writing Information Security Policies by Scott Barman
- ▶ Network Security: The Complete reference Roberta Bragg, Mark Phodes-Ousley, Keith Strassberg



Table of Contents

Volume II

Module 4:	Systems Development Life Cycle & Application Systems	329
1	Business Application Development Framework.....	331
2	Phases In Development of Software.....	353
3	Alternative Methodologies of Software Development.....	371
4	Project Management Tools and Techniques.....	387
5	Auditing the System Development Process.....	397
6	Specialised Systems.....	403
Module 5:	Business Continuity Planning	435
1	Introduction to BCP	437
2	Risk Assessment.....	449
3	Data Recovery.....	455
4	System Recovery	461
5	Contingency Plan Development.....	475
6	Audit and Evaluation of BCP.....	489
Module 6:	Information Systems Organisation & Management	503
1	Information Systems Organization & Management.....	505
2	IT Security and IT Security policies	525
3	Information Systems Management and Controls.....	531
4	IS Management Practices	543
5	IT Change Management.....	555
6	Organization Structure & Controls in IT Department.....	561
Module 7:	IS Audit Process.....	585
1	Information Systems Risks and Controls.....	587
2	Overview of Information Systems Audit	627
3	Information Systems Audit Performance.....	643
4	IS Audit Techniques & CAAT.....	687
5	Overview of ISAudit and Related Standards.....	725
Glossary		759



Module 4:

Systems Development Life Cycle & Application Systems

1 Business Application Development Framework

✂ Learning Goals ✂

A clear understanding of:

1. The need for structured system development
2. The various phases of SDLC and their interrelationship in brief
3. Feasibility Study
4. System Requirement Analysis
5. Hardware and software acquisition
6. People involved in SDLC and their roles and responsibilities

Business Application Development involves

1. Developing, acquiring and maintaining the application systems that are critical to the Business Processes.
2. The effective management and control of the critical business systems and they often control critical information assets.
3. The SDLC involves the defined phases and it is an incremental step for the next phase in building and operating business application systems.

The system development life cycle projects are initiated when a business organization visualized one or more of the following situations:

- a. A new business application is required to be developed to address a new or existing business.
- b. Adoption of a new technology invented or available becomes advantageous to the business.
- c. The application software to be developed, is expected to rectify the present problem related to existing business and
- d. The application software to be developed, is expected to rectify the present problem related to existing technology

In short, system development life cycle commences either with visualizing the benefit of the new software for either to run a new business or the new technology or to have the present problems with business process or with the existing technology to be rectified.

Need for Structured Systems Development Methodology

1. Software is a logical intangible product which makes all the difference in estimating, measuring and managing it without a methodology.
 2. Software products depend heavily on the quality of people carrying out system development, therefore, clear procedures for the development are required to be communicated and followed by the concerned employees. This helps in a better planning and control by the project managers on cost and delivery time and compliance to the standards and quality by the developers.
- ▶ Without proper and adequate planning, design and testing at the appropriate times for the functionality and controls, the software may not satisfy the user's needs, and without adequate control framework, leading to vulnerabilities for the business processes.

SDLC and related risks

The SDLC framework provides system designers and developers to follow a sequence of activities. The advantages of this system are:

- ▶ Better planning and control by project managers
- ▶ Compliance to prescribed standards ensuring better quality.
- ▶ Documentation that SDLC stresses on is an important measure of communication and Control.
- ▶ The phases are important milestones and help the project manager and the user for review and signoff.

Risks associated with SDLC

The shortcomings of SDLC are as follows:

- ▶ The development team may find it cumbersome.
- ▶ The users may find that the end product is not visible for a long time.
- ▶ The rigidity of approach may prolong the duration of many projects.
- ▶ IT may not be suitable for small and medium sized projects.

A well structured systems and methodology for the development of the systems has the following distinct processes:

1. Detailed documentation identifying the need or problem for the development of software
2. Specifying the system to be developed
3. The potential benefits resulting from the development of the new system.
4. Identification and evaluation of both external and internal factors affected by the problem and their effect on the business.

From the perspective of the IS Audit, the following are the possible advantages:

1. The IS Auditor can have clear understanding of the various phases of the SDLC on the basis of the detailed documentation created during each phase of SDLC.
2. The IS auditor on the basis of his examination, can state in his report about the compliance by the IS management of the procedures, if any, set by the management.
3. The IS auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
4. The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

Overview of Phases in Structured Methodology of SDLC

The traditional SDLC has the following seven sequential phases. Each of the earlier phase provides a basis for the subsequent phase of SDLC.

The traditional SDLC approach involves the following phases:

PHASE NO.	PHASE NAME	NATURE OF ACTIVITY
1	Feasibility Study	Determining and evaluating the strategic benefits of the system and ensure that the solution fits the business strategy. Includes cost-benefit analysis of the proposed system.
2	System Requirement Analysis	Analyzing the type of the system on the basis of the users requirements.
3	Design	Designing the system in terms of user interface, data storage and data processing functions on the basis of the requirement phase by developing the system flow charts, system and data flow diagrams, screens and reports etc.
4	Development / Programming	Programming the system as designed and conduct the continuous testing and debugging.
5	Testing	Various kind of testing is conducted before the developed system is implemented. The testing include Unit testing, Integration testing and system testing etc.

PHASE NO.	PHASE NAME	NATURE OF ACTIVITY
6	Implementation	Final testing and quality and controls audit, acceptance by management and user before migration of the system to the live environment and data conversion from legacy system to the new system.
7	Post Implementation	Continuous evaluation of the system as it functions in the live environment and its updation.

Primary Phases in SDLC

Phase 1: Feasibility Study:

Determine and analyse the strategic benefits in implementing the system through evaluation and quantification of:

- a. Productivity gains
- b. Future cost avoidance
- c. Cost savings
- d. Intangible benefits like improvement in morale of employees

This phase justifies the proceeding to the next step.

The following is typically addressed in the Feasibility Study:

- 1. Determine whether the solution is as per the business strategy.
- 2. Determine whether the existing system can rectify the situation without a major modification
- 3. Define time frame for which the solution is required
- 4. Determine the approximate cost to develop the system
- 5. Determine whether the vendor product offers a solution to the problem

The steps involved in the feasibility study phase are:

- 1. Identification of problem
- 2. Identification of objective
- 3. Delineation of scope
- 4. Feasibility study

1. Identification of problem

The first step in application development is to define the problem clearly and precisely. This can be done only after several rounds of discussions with the user group. Then its prevalence within the organisation has to be assessed. A problem that has a considerable impact on the organisation is likely to receive immediate management attention. User involvement will also be high, if they are convinced that the proposed solution will resolve the problem.

2. Identification of objective

After the problem has been identified, it is easy to work out the Objectives of the proposed solution. For instance, inability to provide a convenient reservation system for a large number of intending passengers was the problem of the Railways. So its objective was 'to introduce a system wherein intending passengers could book a ticket from source to destination, faster than in real-time'.

3. Delineation of scope

The scope of a solution defines its boundaries. It should be clear and comprehensible to the user management, stating what will be addressed by the solution and what will not. Often the scope becomes a contentious issue between development and user organisations. Hence, outlining the scope in the beginning is essential.

The following questions should be answered while stating the scope:

- ▶ **Functionality requirements:** What functionalities will be delivered through the solution?
- ▶ **Data to be processed:** What data is required to achieve these functionalities?
- ▶ **Control requirements:** What are the control requirements for this application?
- ▶ **Performance requirements:** What level of response time, execution time and throughput is required? (For customers interacting directly with application programs, the acceptable response time must be specified. Similarly, in the case of large-volume transaction processing applications, batch-processing time may be a limiting factor.)
- ▶ **Constraints:** What are the conditions the input data has to conform to? For example, what is the maximum number of characters that a name can have in a database? This needs to be addressed, because some constraints may affect the implementation of a solution. Conversely, the solution may have to be restructured, taking into account constraints.
- ▶ **Interfaces:** Is there any specific hardware / software that the application has to interface with? For example, payroll application may have to capture data from the attendance monitoring system that the company has already installed. Then the solution developer has to understand the format of data, frequency mode of data transfer and other aspects of the software.
- ▶ **Reliability requirements:** Reliability of an application is measured by its ability to remain uncorrupted in the face of inadvertent / deliberate misuse. The reliability required for an application depends on its criticality and the user profile. For instance, an ATM application should protect the database against any misuse.

Module 4, Chapter 1

Here are a few aspects that have to be kept in mind while eliciting information to delineate the scope:

- ▶ Different users will represent the problem and required solution in different ways. The systems developer should elicit the need from the initiator of the project, alternately called champion or executive sponsor of the project. Addressing his concerns should be the basis of the scope.
- ▶ While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organisation. An understanding of their profile helps in designing appropriate user interface features.
- ▶ While presenting the proposed solution for a problem, the development organisation has to clearly quantify the economic benefits to the user organisation. The information required has to be gathered at this stage. For example, when you propose a system for Road Tax Collection, data on the extent of collection and defaults is required, to quantify benefits that will result to the Transport Department.
- ▶ It is also necessary to understand the impact of the solution on the organisation - its structure, roles and responsibilities. Solutions, which have a wide impact, are likely to meet with greater resistance. ERP implementation in organisations is a classic example of change management requirement. Organisations that have not been able to handle this have had a very poor ERP implementation record, with disastrous consequences.
- ▶ While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weightage too. These factors have to be considered from the perspective of the user management and resolved. For example, in a security system, how foolproof it is, may be a critical a factor like the economic benefits that entail.
- ▶ Unless it is a greenfield project, some organisational processes may already be computerised, and the present solution will have to co-exist with these applications. So, an understanding of the existing environment will make it easier to define the scope.
- ▶ A list of the user performance expectations will make outline the scope easier and more focussed.
- ▶ Interviews / discussions at this stage should also elicit the factors, that are likely to constrain the proposed solution.

4. Feasibility study

Technical Feasibility

Despite rapid growth in technology, there are many areas that haven't benefited much from the existing technology. For example, a bank may desire to cut down the input time of drafts for reconciliation purposes by scanning them. However such output is generally in the form of bit maps. Matching figures in these scanned documents through OCR

(Optical Character Recognition) technology is still feasible only with printed documents-that too with selected fonts only.

Financial feasibility

The solution proposed may be prohibitively costly for the user organisation. Monitoring stock through the VSAT network connecting multiple locations may be acceptable for an organisation with high turnover. But this may not be a viable solution for smaller ones.

Economic feasibility

Cost / Benefit analysis is an important tool for feasibility study. This requires all the costs and benefits to be quantified, and only if the benefits exceed costs, the solution is deemed feasible.

The Net Present Value (NPV) technique is used for cost / benefit analysis. In cases, where the benefits cannot be easily assessed in the initial stage, Keen's value analysis is recommended. In this approach seed funding is allocated to build a prototype. With the prototype, users are expected to have a better idea of the benefits. At this stage, if the estimate of benefits exceed costs, additional funding is allocated and the product / prototype building is continued. Thus the process continues, with assessment of estimated costs and benefits at each iteration.

Time feasibility

If the benefit of a solution can be derived only when it is implemented within a specified time, then the solution should be assessed on the feasibility of meeting this crucial time target. Organisations that had not taken up the Y2K conversion before 1999 opted for a new Y2K compliant solution. This seemed better than converting their legacy application, because there was not much time to do so.

Resources feasibility

Since financial resources have already been dealt with, here the focus is on human resources. Implementing sophisticated software solutions becomes difficult in non-metro locations. This is because of the reluctance of skilled personnel to move to such locations.

Operational feasibility

A good system can be designed to process data and produce the desired outputs. However, if the data input for the system is not readily available or collectable, then the system may not be successful. This factor too must be considered.

Behavioural feasibility

Systems, which will have an adverse effect on the quality of work life, should also be considered unviable. Computerisation itself has been the casualty of the perceived threat of unemployment in the initial years.

Legal feasibility

Any system, which violates the local legal requirements should also be rejected. While high resolution scanning and printing may render duplication of currency notes technically feasible, it is not legally admissible !

Phase 2: System Requirement Analysis:

On the basis of the user needs, the problem or need that requires resolution is defined and decision on customized or vendor supplied software, involving defined and documented acquisition process.

The following are the steps undertaken in the requirements phase:

- a. Identify and consult the stakeholders to determine their expectations and resolve their conflicts
- b. Analyse requirements to detect and correct conflicts and determine priorities
- c. Identify how the system should interact with its environment
- d. Convert the user's requirement into system requirement by showing the users interactive prototypes.
- e. Record requirements in a structured format, which should be in writing and possibly in schematic models.
- f. Verify the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable.
- g. Resolve conflicts between the requirements set and the resources that are available.

From the interactive process, a general preliminary design of the system may be presented to the user management for their modification, approval and endorsement.

The commitments are obtained from the user departments and system developers to contribute the necessary resources to complete the project.

To design a new system, first it is essential to understand the existing system. An analysis should include

1. A study of the existing organisational history, structure and culture
2. A study of the existing information flows

Study of history, structure and culture

The study of the history of systems in an organisation gives an idea of: the types of systems that have been extremely useful; issues that have not been addressed over a period; and new issues that require attention.

The organisational structure gives an idea of the power equations within an organisation. An understanding of the organisational culture is possible by talking to users. Sometimes they may be guarded, but experienced systems analysts can read between the lines. Solutions that are not consistent with the culture often fail. To cite an example, one of the

benefits of ERP systems is empowerment of employees. However, since many Indian organisations have pyramidal structures, users do not construe this as a benefit.

Study of information flows

Normally, the new information flow merely involves tweaking the existing flow. Weaknesses are worked on, rarely is a radically new information flow developed. Hence, it is essential to study the existing information flow. This can be done using the following approaches:

A. Data flow diagram

Data Flow Diagram (DFD) is a popular tool for analyzing and representing information flow:

A DFD has four elements:

1. Data Flow: represented by arrow
2. Process: represented by circle (bubble) or rectangle with rounded edges
3. Data Stores: represented by parallel lines or open rectangle
4. External Entity: represented by square

Rules of DFD

- ▶ All entities, processes and data stores should be numbered and named.
- ▶ It is preferable to mention the data flowing on the arrows too.
- ▶ DFD is always read from top to bottom and left to right.
- ▶ No more than seven processes (five is ideal) should be represented in the same page. In case there are more processes - in real life there will be - first gross level processes should be shown. This can later be broken down.

Limitations of DFD

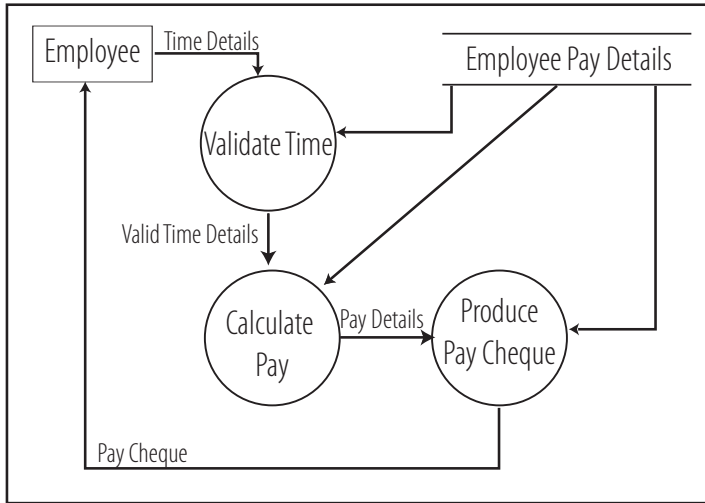
- ▶ It is not possible to represent conditions and decisions (as in flow charts) in DFD.
- ▶ DFDs do not show the time intervals or delays between processes.

At the lowest level of bubbles, the processing logic may have to be explained- in such a case, DFD is not a good tool.

Four other techniques are used for this:

- ▶ Flow Charts
- ▶ Decision Trees
- ▶ Decision Tables
- ▶ Structured English

Data Flow Diagram



B. Flow chart

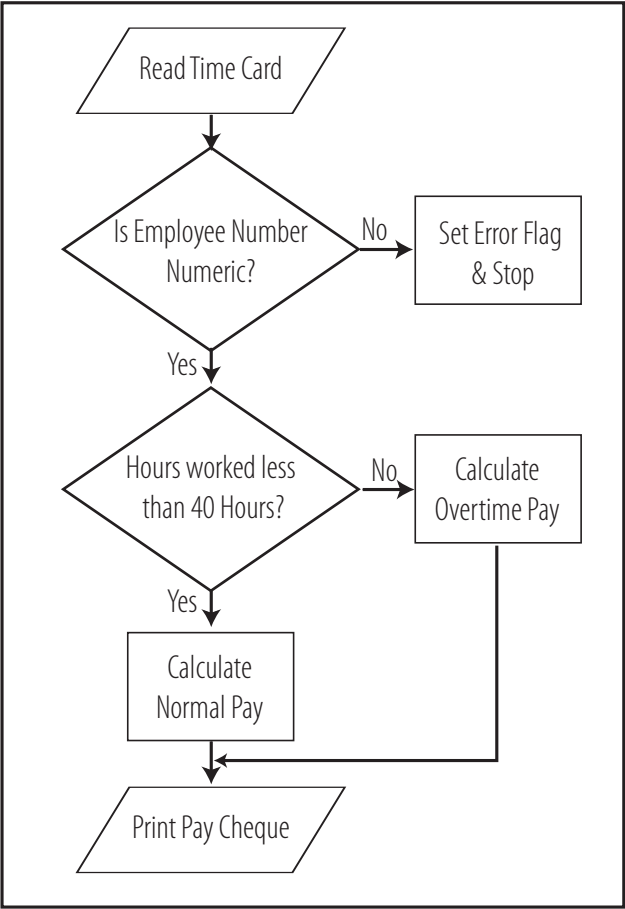
Flow chart is the most widely-used method for representing logic. In a flow chart,

- ▶ A circle represents start and stop
- ▶ A box represents a processing step
- ▶ A rhombus represents a logical condition
- ▶ An arrow represents the flow of information

The three structured constructs are represented in a Flow Chart in the following manner:

- ▶ Two processing boxes connected by an arrow represent sequence.
- ▶ A diamond represents condition. It has two paths, one for the condition being true, another for it being false
- ▶ A loop represents repetition

Flow Chart Diagram



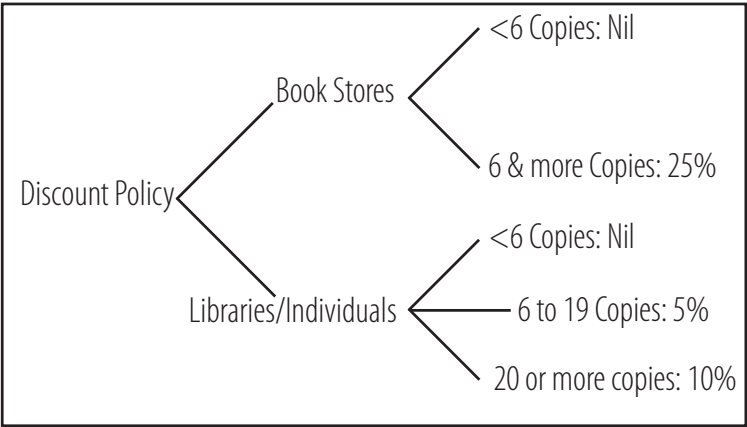
C. Decision tree

When multiple conditions operate, the decision tree is a better option. Consider the following example:

Bookstores get a trade discount of 25% for 6 copies or more. For orders from libraries and individuals; a discount of 5% is allowed on orders of 6 -19 copies per book title, 10% on orders of 20 or more copies per book title.

The decision tree for representing the discount policy is as follows:

Decision Tree Diagram



D. Decision table

When a set of complex conditions needs to be evaluated for selecting appropriate action, then the decision table is the preferred option. The decision table provides conditions and actions in a tabular form.

The decision table is divided into four quadrants. The upper left quadrant contains all conditions. The lower left quadrant contains actions that are possible for each combination of conditions. Values for all the possible combinations of a given set of conditions and the corresponding event (or action to be taken) are stored in the right quadrants. Each column in the right quadrant can be interpreted as a processing rule.

Let us illustrate this with an example:

Electricity consumers are charged tariffs on the following basis: Low-end consumers are charged at the rate of Re. 1 per unit, if their consumption is less than or equal to 100 units per month. However, if their consumption is more than 100 units per month, then they will be charged at Rs. 2 / unit. For high-end consumers, the charges are Rs. 2 / unit, if their consumption is less than or equal to 100 units per month; if their consumption is more than 100 units per month they are charged at Rs. 3/unit.

This example is illustrated in the decision table given below:

Particulars		1	2	3	4
Conditions	Low tension/low-end consumers	T	T	F	F
	High tension/high- end consumers	F	F	T	T
	Consumption < = 100 units	T	F	T	F
	Consumption> 100 units	F	T	F	T

Particulars		1	2	3	4
Actions	Re. 1 / unit	X			
	Rs. 2 / unit		X	X	
	Rs. 3 / unit				X

E. Structured English

Structured English is also known as Program Design Language (PDL) or Pseudo code. In this method, the logic can be represented in English, but the syntax is very similar to programming languages — the number of words is limited to convey the precise meaning.

E.g.:

MULTIPLY HOURS-WORKED BY PAY-RATE TO GET GROSS-PAY

IF condition-1 THEN action -A ELSE action - B

REPEAT < > UNTIL <condition>

System Specification

At the end of the analysis phase, the systems analyst prepares a document called Systems Requirement Specifications (SRS). A suggested format for this document:

- ▶ Introduction
 - ▼ Goals and objectives of the software Context of the computer-based system
 - ▼ Information description
- ▶ Information description
 - ▼ Problem description
 - ▼ Information content, flow and structure
 - ▼ Hardware, software, human interfaces for external system elements and internal software functions.
- ▶ Functional description:
 - ▼ Diagrammatic representation of functions
 - ▼ Processing narrative for each function
 - ▼ Interplay among functions
 - ▼ Design constraints
- ▶ Behavioural description:
 - ▼ Response to external events and internal controls
- ▶ Validation criteria:
 - ▼ Classes of tests to be performed to validate functions, performance and constraints
- ▶ Appendix:
 - ▼ Data flow / Object diagrams

Module 4, Chapter 1

- ▼ Tabular data
- ▼ Detailed description of algorithms Charts, graphs and other such material

Specification review

The SRS document is reviewed by the user / customer. Normally, first the development team makes a presentation / organisation and then the document is handed over. This helps users to understand the document better.

The user should carefully review the SRS document, because it reflects the development team's understanding of the existing processes. Any misconception at this stage can lead to problems in design and development. Only after ensuring that the document represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organisation.

Software Acquisition

Software acquisition is not a phase in standard SDLC. But if the business has decided to acquire the software rather than developing the same, software acquisition is the process which should occur after Requirement Analysis Phase. The following steps shall be relevant in acquisition of the software.

1. The feasibility study in relation to the software acquisition should contain documentation that supports the decision to acquire the software.
2. The decision is based upon various factors like Cost difference between development and acquisition, availability of the required software readily in the market, the time saved between development and acquisition etc.
3. A project team comprising of technical supports staff and key users should be crated to prepare Request for Proposal (RFP).
4. The project team should carefully compare and examine the various responses of the Vendor to the RFP , prepare the gap analysis and shortlist the vendors on the basis of such evaluation.

Contents of Request for Proposal:

ITEM	DESCRIPTION
Product Vs System requirements	1. Comparison between the required system and the vendor developed product – to include the volume of transactions that the software can handle and the database size. 2. Acceptance or otherwise from the users for the deficiencies in the vendor product. 3. Possibility of the customization by the Vendor to address the deficiencies
Customer References	Validate the Vendor's claims about their product performance and timely completion of work by the vendor from the Vendor's customers.
Vendor's viability and financial stability	Evaluate the vendor's viability with reference to period for which the vendor is in operation, the period for which the desired product is being used by the existing customers and the Vendor's financial stability on the basis of the market survey and the certification from the customers and on certain supporting documentation from the Vendor .
Availability of complete and reliable documentation about the new software	Review the complete set of system documentation provided by the Vendor prior to acquisition of the software. The documentation should be in detail and precise.
Vendor Support	Evaluate what kind of support the vendor provides for the software like onsite maintenance, online updation of upgrades, onsite training to users, automatic new version notifications, 24 x 7 Helpline etc.
Response time	Time taken for the vendor to respond and fix in case a problem is reported.
Source Code Availability	1. If the software is developed only for the concerned business, with the vendor has no right for a further sale, the source code must be given by the Vendor. 2. In other case, the source code should be deposited with a third party so that the same would be available if the vendor goes out of business. The source code with the program updates and program fixes should be included as a part of escrow agreement.
Vendor's experience	Vendor having longer experience in the desired software is more acceptable

ITEM	DESCRIPTION
A list of recent or planned enhancements to the product with the dates	This will ensure the vendors effort to keep the product current.
List of current customers	More the number of customers, more is the acceptability of the product.
Acceptance testing of product	The vendor should allow the acceptance testing by the users to ensure that the product satisfies the system requirements of the business. This should be done before purchase commitment.

- 5. The project team should invite the short listed vendors to have presentation of the product and the processes. The users participation with feedback must be ensured in such presentation. The project team may also visit some of the customers to have live demonstration of the software. The discussion with the customers should focus on:
 - i. Reliability of the Vendor's deliverables
 - ii. Vendor's commitment to service to sort out the system problems
 - iii. Vendor's commitment to user training and system documentation
- 6. Once the final vendor is confirmed, the vendor should be invited to present a pilot session so as to enable the project team to understand the system, have a hands on experience and suggest for the areas of customization.
- 7. On the basis of the above activities, the vendor's presentations and final evaluation, the project team can make the final selection of the product.
- 8. The last step in the acquisition process is the negotiation and signing of a legal contract with the vendor. Contract should contain the following items:
 - a. Specific description of the system deliverables and their respective costs
 - b. Commitment dates for their delivery in the order of priority decided by the purchaser
 - c. Commitments for delivery of documentation, fixes, upgrades, new release notification and training to the purchaser
 - d. Allowance of escrow agreement if the deliverables do not include source code.
 - e. Description of the support to be provided during installation on site.

- f. Provision for a reasonable period of acceptance, before purchase is made
 - g. Allowance for changes to be made by the customer company
 - h. Maintenance agreement with the specified period and the maintenance cost
 - i. Payment schedule for the software should be linked to actual delivery dates
9. Managing and control on the implementation of the system is required with the regular status reports.
10. IS auditors job in the software acquisition process would be to determine whether adequate level of security controls has been considered prior to making an agreement. This is required to ensure data integrity of the information processed and controls like audit trails, password controls and overall security of the application.

The above procedures should be more elaborate and systematic in case where the business is implementing ERP systems giving fully integrated corporate solutions like SAP, Oracle Financials, BAAN, PeopleSoft, JD Edwards etc.

Roles Involved in SDLC

Steering committee

Wherever large-scale application development is undertaken, a steering committee is set up to supervise and direct the projects. Normally, this committee is headed by a representative from the top management, to act as a Chairman of the Steering Committee for its meetings, and consists of Senior Manager of each of the affected function the Project Manager as a co-ordination link.

The functions of Steering Committee are:

- ▶ To Provide overall direction and ensures appropriate representation of affected parties
- ▶ To be responsible for all cost and timetables
- ▶ To conduct a regular review of progress of the project in the meetings of steering committee which may involve co-ordination and advisory functions, Taking corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.

Project manager

A project manager is normally responsible for more than one project and liaisons with the client or the affected functions. This is a middle management function, and he is responsible for delivery of the project within the time and budget. He periodically reviews the progress of the project with the project leader and his team. Project leaders report to him. He appraises the Steering Committee about the progress of the work.

Module 4, Chapter 1

Project leader

He is dedicated to a project and has to ensure its completion and fulfillment of objectives. The entire project team reports to him. He reviews the project position more frequently than a Project Manager.

Systems analyst

The systems analyst is also referred to as a business analyst. His main responsibility is to conduct interviews with users and understand their requirements. He is a link between the users and the programmers. He converts the users requirements in the system requirements. He plays a pivotal role in the Requirements analysis and Design phase.

Module leader / Team leader

A project is divided into several manageable modules, and the development responsibility for each module is assigned to module leaders. For example, while developing a financial accounting application – Treasury, Accounts payable, Accounts receivable can be identified as separate modules and can be assigned to different module leaders. These module leaders will have programmers reporting to them. Module leaders are responsible for the delivery of tested modules within the stipulated time and cost.

Programmers

Programmers are the masons of the software industry. They convert design into programs by coding using programming language. They are also referred to as coders or developers. Apart from developing the application in a programming language, they are also responsible for first level testing of the programs they develop and debugging activity.

Database Administrator (DBA)

Module leaders and programmers are responsible for the process side of the application. As for data definition, this is done by the system designer (Ron Weber assigns this to a data administrator; but such a role is non-existent in Indian organisations). The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The database administrator handles multiple projects; he ensures the integrity and security of information stored in the database. He also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.

Quality assurance

This team sets the standards for development, and checks compliance with these standards by project teams on a periodic basis. The team is the same for all projects. Any quality assurance person who has partici-

pated in the development process shall not be viewed as “independent” to carry out quality audits.

Testers

Testers are junior level quality assurance personnel attached to a project. They test programs and subprograms as per the plan given by the module / project leaders and prepare test reports.

Domain specialist

Whenever a project team has to develop an application in a field that's new to them, they take the help of a domain specialist. For example, if a team undertakes application development in Insurance, about which they have little knowledge, they may seek the assistance of an Insurance expert at different stages. This makes it easier to anticipate or interpret user needs. A domain specialist need not have knowledge of software systems.

Technology specialist

IT is developing so rapidly that even IT professionals find it difficult to keep track of all developments, let alone develop expertise. This has resulted in experts in specific technology areas, such as Microsoft technology, Web-enablement and the like. If the application development team needs guidance in any of these areas, then it could associate with experts on a part- time basis.

Documentation specialist

These professionals are responsible for the creation of user manuals. They are expected to understand the functions of the software, and provide documentation that makes it easy for the user also to do so. They should also have a good command of the English language, and be able to simplify complex concepts. Technical writing is an emerging field in India. In many organisations programmers or module leaders also wind up doing this job, and this affects the quality of the document.

In many organisations, some of these roles may be integrated into a single role. Sometimes, depending on the skill level, individuals may be required to perform more than one role. However, quality assurance personnel should not be stretched to take on other responsibilities.

IS auditor

Should the IS auditor be part of the development process? As a member of the team, he can ensure that the application development also focuses on the control perspective. He should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.

Summary

Complete designing and implementation of a system entails both software development and hardware implementation. However, a substantial portion of the cost incurred in application development is in designing and developing software.

People now view system development as a methodical and planned sequence of developmental phases. Thus, typically a comprehensive and exhaustive approach to system development has three developmental phases:

1. System definition that focuses on:
 - ▼ What the problem is
 - ▼ What the desired functions are
 - ▼ What data has to be processed
 - ▼ What level of performance is desired
 - ▼ What system behaviour can be expected
 - ▼ What interfaces have to be established
 - ▼ What the design constraints are
 - ▼ What validation criteria are required
2. System development and system support that focuses on:
 - ▼ How to structure data
 - ▼ How to implement the desired functions
 - ▼ How to implement procedural details
 - ▼ How to establish interfaces
 - ▼ How to translate the design into a program
 - ▼ How to perform testing
3. System support that focuses on issues pertaining to repair and maintenance of the product. It also deals with frequent changes made to the product after its delivery. This phase begins with the Implementation phase and continues through the maintenance phase.

The traditional approach to structured application development methodology has been refined and is referred to as the System Development Life Cycle (SDLC). It has seven phases: Feasibility Study, System Requirement Analysis, Design, Programming, Testing, Implementation, and Post Implementation Review.

System Development Life Cycle often referred to as SDLC, is a systematic and structured process for developing information systems. It has seven developmental phases viz., feasibility study, requirement analysis, system design, program construction, testing, implementation and post implementation review. Each of these stages of application development consists of several multiple stages.

Feasibility study assesses how viable or how feasible it is to develop the system. This includes defining the system, understanding the objectives, delineating the scope and presenting a study of the technical, financial, operational, behavioural and legal feasibility of the system.

The next step that follows is the system requirement analysis. Two major tasks involved in requirement analysis are:

- ▶ Studying the existing organisational history, structure and culture
- ▶ Studying the existing information flows

The various people involved in SDLC are project manager, project leader, systems analyst, module leader/team leader, programmers, database administrator, quality assurance, personnel, testers and documentation specialists. Apart from these people in a typical process, the IS auditor also plays a critical role. He brings in a control perspective to the application development. An auditor should be aware of the changes made during the process of application development.



2 Phases In Development of Software

✂ Learning Goals ✂

A clear understanding of all the phases of SDLC except the phase involving feasibility study and system requirement analysis.

System Design Phase

Based on the requirements definition, the system shall be designed . The system design will:

1. describe the parts of the system and their interaction
2. set out how the system shall be implemented using the chosen hardware, software and network facilities
3. specify the program and the database specifications and the security plan
4. specify the change control mechanism to prevent uncontrolled entry of new requirements.

Users may not be involved in this phase as they may not know the technicalities.

Key design phase activities include:

- A. Developing system flowcharts to illustrate how the information shall flow through the system
- B. Defining the applications through a series of data or process flow diagrams, showing various relationships from the top level down to the detail.
- C. Describing inputs and outputs, such as screen design and reports.
- D. Determining the processing steps and computation rules for the new solution
- E. Determining data file or database system file design
- F. Preparing the program specifications for the various types of requirements or information criteria defined
- G. Developing test plans for:
 - i) Unit (Program) Testing ii) Subsystem (Module) Testing iii) Integration (System) testing iv) Interface with other systems v) Loading and initializing files vi) Security, backup and recovery
- H. Developing data conversion plans to convert data and manual procedures from the old system to the new system.

Module 4, Chapter 2

After the detailed design phase is completed, the design is then distributed to the system developers for coding.

This phase deals with the way the proposed system can be transformed into a working model. The steps involved in this phase are:

1. Architectural design
2. Design of data / Information flow
3. Design of database
4. Design of user interface
5. Physical design
6. Selection of appropriate hardware and software

Architectural design

Architectural design deals with the organisation of applications in terms of hierarchy of modules and sub-modules. At this stage, we identify:

- Major modules
- Function and scope of each module
- Interface features of each module
- Modules that each module can call directly or indirectly
- Data received from / sent to / modified in other modules

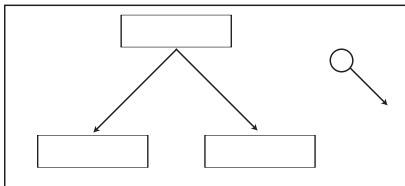
The architectural design is made with the help of a tool called functional decomposition.

Functional decomposition

This tool can be used to represent hierarchies. It has three elements:

- Module
- Connection
- Couple

The module is represented by a box. The connection between modules is represented by arrows. Couple is the data element that moves from one module to another. It is represented by an arrow with circular tail.



Design of data / Information flow

In designing the data / information flow for the proposed system, the following inputs are required:

- Existing data / information flows
- Problems with the present system
- Objective of the new system

All these have been identified in the analysis phase and documented in Software Requirements Specification (SRS). For representing the new design, we use the same tools that were used in analysis phase: Data Flow Diagrams (DFDs) or object-oriented notations. Apart from the flow of data, the frequency and timing of flow are also identified in this stage. For example, in an organisation invoice data is received from branches every day, but the consolidation process (documentation) is done on a weekly basis, say on Friday. The data flow should also be documented at every stage.

Design of database

At this stage, the scope and structure of the database is decided. A decision is also taken whether to opt for a centralised or distributed database. This is based on the level of interdependence among organisational units.

The design of the database consists of four major activities:

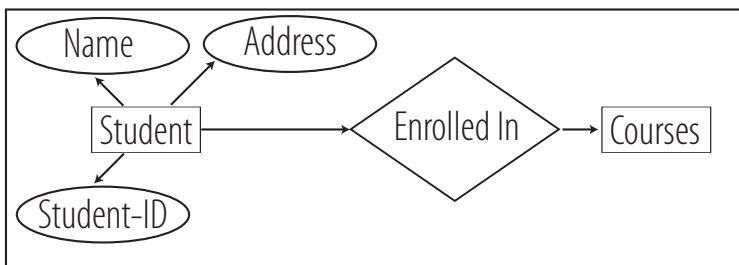
- A. Conceptual modeling
- B. Data modeling
- C. Storage structure design
- D. Physical layout design

Conceptual modeling

In this activity, the application is modeled in terms of entities / objects and their relationships. Every object or event in the system is known as an entity. For example, employee record. The normal practice is to advise the systems analyst to list all nouns from their user interviews, such as: supplier, purchase order, item schedule and the like. All these will be entities in a Purchase System.

Attributes are the characteristics of an entity: Color is the attribute of entity car; qualification is the attribute of entity employee. The relationship between entities is modelled in the Entity -Relationship diagram: Purchase order is raised on supplier; purchase order contains items.

Entity Relationship Diagram



The relationship is further qualified as one-to-one, one-to-many and many-to-many. For example, the relationship between supplier and pur-

Module 4, Chapter 2

chase order is one-to-many. While the relationship between purchase order and item is many-to-many.

For effective and efficient querying, many-to-many relationships are difficult to handle. These relationships are converted into one-to-many by introducing additional entities. The many-to-many relationship between purchase order and item is changed into one-to-many by introducing a compound entity called purchase order-item.

Data modelling

Conceptual models have to be translated into data models, so that they can be manipulated using programming languages. Currently, the most popular data model is relational model, in which data is represented in tables. Every entity identified in the conceptual model is converted into a table, and the attributes are converted into fields (columns in the table).

EMP NAME	EMP ID
Kamalakar	A1005
Prafulla	A1006
Vinod	A1007

A record design technique called normalisation is used to avoid update anomalies. The following are the most common three normal forms:

In the first normal form, the repeating groups in a record are removed and made into a separate record.

For example, in the purchase order record-item no, item description, unit of measure, quantity, rate and amount will repeat as many times as the number of items in the purchase order. This will obviously create inefficiency. Not only will space be wasted because of the duplication of repeating items in each record, but it will take a lot of work to maintain data consistency. For example, if there are 20 items on the purchase order, and one of the repeating fields, say the shipping address, changes, the change will have to be made in each of the 20 records. If the repeating fields (of which the shipping address is one) are made into a one table, and the order details kept in another, there will be only one record in the first table for the order , and space will be used only once for storing this information. Also, the change in the shipping address will only have to be made once, in this record, since the shipping address will no longer be in the second table.

In the second normal form, a check is done on all non-key elements to ensure that they are dependent on the key Continuing with the same example of purchase order record, all supplier-related details will be

moved to a separate supplier table in the second normal form. This is because supplier details are all dependent on supplier code and not on the key of purchase order record, viz. purchase order no.

In third normal form, a check is done to ensure that no non-key element is transitively dependent on another non-key element. For example, discount may be a data element in purchase order. If the discount the supplier offers depends on the amount of purchase Order, it is better to keep discount in a separate table called supplier-purchase order amount.

Storage structure design

During this activity, a decision is made on how to store the data structure on some device.

Physical Layout Design

It is at this stage that detailed physical implementation to the level of cylinders and tracks for the storage of the data is planned.

Design of user interface

Some points that should be considered while designing the user interface design:

- ▶ Level of user - educational background, computer exposure
- ▶ Source document format
- ▶ Output requirements
- ▶ Enquiry screens
- ▶ Graphic and color displays
- ▶ Requirement for special input / output device

Prototypes can be used to elicit user feedback and refine the user interface.

Physical Design

At this stage, the logical design is converted into physical implementation units.

Some of the issues addressed here are:

- ▶ Type of hardware for client application and server application
- ▶ Operating systems to be used
- ▶ Type of networking
- ▶ Processing -batch-online, real-time
- ▶ Frequency of input, output
- ▶ Month-end cycles / periodical processing

Design Principles

The following principles should be kept in mind, while designing the system:

Module 4, Chapter 2

- ▶ There is a tendency to develop merely one design and consider it the final product. However the recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria.
- ▶ The design should be based on the analysis.
- ▶ The software functions designed should be directly relevant to business activities.
- ▶ The design should follow standards laid down. For instance, the user interface should have consistent colour scheme, menu structure, location of error message and the like.
- ▶ The design should be modular.

Modularity

A module is a manageable unit performing a well- defined task. Each module contains data and instructions for the task. Modules have well-defined interfaces. Interaction among modules is based on interfaces,. A modular design results in easy maintainability, and hence it is recommended. Modularity is measured by two parameters: Cohesion and Coupling

Cohesion

Cohesion refers to the manner in which elements within a module are linked. A module that performs one discrete task is said to be more cohesive than a module that performs multiple tasks. Cohesion reflects the strength of bonding between elements of a module.

Coupling

Coupling is a measure of the interconnection between modules. It refers to the number and complexity of connections between 'calling' and 'called' modules.

In a good modular design, cohesion will be high and coupling low.

Development Phase: Programming Methods, Techniques And Languages

The Development Phase starts with the detailed design developed in the Design Phase and begins with coding by using a programming language. The responsibility of this phase is primarily that of the Programmers and System Analysts. The following are the key activities performed during this phase.

1. Coding and developing program and system level documents
2. Testing and debugging continuously for improvements in program developed
3. Developing programs for conversion of the data in the legacy system to new system

4. Formulating the procedures for the transition of the software by the various users
5. Training the selected users on the new system
6. In case of vendor supplied software, documenting the modifications carried out to ensure that future updated versions of the vendor's code can be applied.

A good program should have the following characteristics:

- ▶ **Accuracy:** Accuracy does not only mean that the program should do what it is supposed to do; it should also not do what it is not supposed to do. In fact, the second part becomes more challenging for quality control personnel and auditors
- ▶ **Reliability:** The program keeps doing the same consistently over a period, Since programs do not wear and tear, reliability is taken for granted. However, poor setting of parameters and hard coding some data, which is of temporary value could result in the failure of a program after some time,
- ▶ **Robustness:** In normal circumstances, most programs work, It is extraordinary circumstances that really differentiate the good programs from the bad ones. This means that the programmer has anticipated even the least likely situations and provided safeguards for them, so that mishaps can be avoided, This process of taking into consideration all possible inputs and outcomes of a program is also known as error / exception handling process,
- ▶ **Efficiency:** Performance should not be unduly affected with the increase in input volumes.
- ▶ **Usability:** A user-friendly interface and easy-to-understand user document is necessary for any program.
- ▶ **Readability:** The program should be easy to maintain even in the absence of the programmer who developed it. The inclusion of comment lines is extremely useful.
- ▶ **Maintainability:** If a program has to be maintained by a programmer other than the one who developed it, it should be developed the modular way.

Programming Methods & Techniques

i) Adoption of the Program Coding Standards

To improve the quality of the software developed and its capability for future maintenance, program coding standards should be used.

- ▶ Coding standards are essential for reading and understanding the program code in simple and clear manner
- ▶ Coding standards may include source code level documentation, methods for data declaration, and technique for input / output.

Module 4, Chapter 2

- ▶ Coding standards serves a method of communication between teams, amongst the members of the teams and the users, thereby working as a good control.
- ▶ Coding standards minimize the system development setbacks due to programmer turnover
- ▶ Coding standards help in efficient program modification and maintenance

ii) Structured programming

This helps in the modular development of the programs. Each module can be independently developed and integrated with the other modules.

The following rules ought to be followed while developing programs:

1. Every program should have only one entry and one exit. This will apply to sub programs within a program also, This makes it easy to communicate the logical flow to other programmers,
2. The program should have only three basic building blocks:- **SEQUENCE, SELECTION** and **ITERATION**. Identification of a small number of building blocks makes programs structured and minimizes the deviations introduced by individual programmers.
3. The GOTO syntax is best avoided in structured programming. GOTO introduces a criss-cross flow in programming, which reduces readability and maintainability.
4. Programs can be developed either top-down or bottom-up.

iii) Online Programming Facilities

To facilitate the effective use of the structured programming techniques, an online programming facility should be allowed. The following are the advantages of this technique.

1. This technique allows programmers more flexibility in coding and compiling the programs with a remote computer.
2. By the use of this facility, the programmers can enter, modify and delete program codes as well as compile and store the programs on the computer
3. This facility, in general, allows a faster development of the programs
4. This approach can lower the development costs, maintain rapid response time and effectively expand the programming resources.

The following are the potential weakness of this facility:

1. Control of multiple versions of the programs
2. Control to unauthorized access and updating of programs
3. Control on proper updating of changes

Programming Language

Application programs are first coded by using the programming language in the form of statements or instructions and the same is converted by the compiler to binary machine language for the computer to understand and execute.

The programming languages commonly used are:

- i. High level general purpose programming language such as COBOL and C language.
- i. Object oriented languages like C++, JAVA etc
- ii. Scripting language like JavaScript, VB Script etc
- iii. Fourth generation high level programming languages (4GLs) like FOCUS, dBase
- iv. Decision support or expert system languages like Express, LISP and PROLOG

Programming languages have also evolved through generations from the machine languages to high level languages.

High level languages such as COBOL and C require programmer to specify the sequence in which the computer will execute instructions to arrive at a result. In other words, these languages require the programmer to specify what he wants to achieve, and how he wants to achieve it. These are called procedural languages.

In fourth- generation languages, a programmer is required to specify only what he wants and not how. That is why these are called non-procedural languages.

Some of the special features of 4GLs are:

- ▶ Their functions can be driven by an event like a mouse click.
- ▶ They are portable across hardware environments.
- ▶ They have highly user-friendly syntax: the syntax is as near English statements as possible.
- ▶ They have utilities for screen painting and report generation.
- ▶ They can produce graphical outputs.
- ▶ They have powerful querying capability.
- ▶ However where response time or batch- execution time is the criterion, they could be somewhat slower.
- ▶ They are not very good in handling a large number of transactions.

1) Choice of programming language

With several programming languages being available today, the choice of language is the first issue that needs to be addressed. The following are among the most important criteria

- ▶ Application area
- ▶ Algorithmic complexity
- ▶ Environment in which software has to be executed
- ▶ Performance consideration
- ▶ Data structure complexity
- ▶ Knowledge of software development staff
- ▶ Capability of in-house staff for maintenance

Module 4, Chapter 2

Many times, the hardware or database may restrict the choice of language.

2) Coding style

Programming can be improved by following the guidelines given below:

- ▶ Consistent and meaningful names for programs, variables and the like improve understandability and maintainability. A trial balance program can be called trialbal rather than Fin32. Similarly, employee number can be referred to as emp_no. In which case, suppliers will be referred to as supp__no. this ensures consistency in naming conventions.
- ▶ Modular programming makes maintainability easy
- ▶ Languages like C permit more than one instruction to be written in a line. But to improve readability 'one instruction per line' standard must be maintained.
- ▶ Comment lines improve the understandability of code. These indicate the function of each logical block. Adequate comment lines should be included in the program
- ▶ Indentation, parenthesis and the like improve readability of the code if the logic is complicated, clear formatting will make it easy to understand.

3) Program Debugging

Debugging is the most primitive form of testing activity. Programmers usually debug their programs while developing their source codes by activating the compiler and searching for implementation defects at the source code level. Bugs (Defects) are always the result of faulty code structure, misunderstanding of the programming language features, incoherent naming or wrongly spelt programming statements.

The need for extensive debugging is often an indication of poor workmanship. Debugging activities should be kept at minimum and the programmer should not entirely be dependent on the compilers but should also take help of the debugging software.

Debugging software tools assist the programmer in fine tuning, fixing and debugging the program under development. These tools fall in the following three categories.

- ▶ **Logic Path Monitors:** provides clues to the programmer on logic errors by reporting on the sequence of events achieved by the program
- ▶ **Trace:** This lists the changes in selected variables at different stages of the program.
- ▶ **Memory Dumps:** provides a picture of the internal memory content at the point where the program has abruptly ended, providing the clues to the programmer on the inconsistencies in data and parameter values.

- ▶ **Output Analyzer:** checks the accuracy of the output which is the result of processing the input through that program by comparing the actual results with the expected results.

Software Testing Phase

Software testing is the process of testing software in a controlled manner to ensure it meets the specifications. During testing, the developer should give up preconceived notions of the correctness of the software developed

Objectives of testing

The following aspects have to be kept in mind while testing:

- ▶ Testing is a process of executing a program to identify an error.
- ▶ A good test case is one that has high probability of finding an error.
- ▶ A successful test is one that uncovers an error.

Levels of testing

Every software normally goes through the following levels of tests:

A. Unit testing

B. System testing

A. Unit testing

Unit testing is the process of testing individual units of software in isolation. A program unit is usually small and the programmer who developed it can test it in great detail. Certainly in greater detail than is possible when the unit is integrated into an evolving software product. It uses a set of test cases that focus on the control structure of the procedural design. These tests ensure that the internal operation of the program performs as per the specification. There are four categories of tests that a programmer typically performs on a program unit:

- ▶ **Functional tests** – These tests check whether programs do what they are supposed to do. The test plan specifies operating conditions, input values, and expected results, then it checks by inputting the values to see the actual result and expected result match.
- ▶ **Performance tests** – These should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilisation and the traffic rates on data channels and communication links
- ▶ **Stress tests** – These are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
- ▶ **Structural tests** – These are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.

Module 4, Chapter 2

- ▶ **Parallel Tests** – By using the same test data in the new and old system, the output results are compared.

Types of unit tests

Static analysis tests

Some important static analysis tests are:

- ▶ **Desk Check:** This is done by the programmer himself. He checks for logical syntax errors, and deviation from coding standards.
- ▶ **Structured walk-through:** The application developer leads other programmers through the text of the program and explanation
- ▶ **Code inspection:** The program is reviewed by a formal committee. Review is done with formal checklists. The procedure is more formal than a walk-through.

Dynamic analysis tests

- ▶ **Black Box Test:** After understanding the specified function that a product has been designed to perform, tests can be conducted to check whether each function is fully operational. In other words, the focus is on functional correctness. This is known as black box testing. If a module performs a function it is not supposed to, the black box test does not identify it.
- ▶ **White Box Test:** After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised. In other words, the focus is on structural correctness. This is called white box testing. White box test will not verify if the module performs all the functions that it is supposed to perform.

Integration / Interface testing:

The objective is to evaluate the connection of two or more components that pass information from one area to another. This is carried out in the following manner.

- ▶ **Bottom-up integration:** Bottom-up integration is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub-system testing, and then testing of the entire system. Unit testing has to uncover errors in the individual modules of the system. Sub-system testing checks the operation of the interfaces between modules in the subsystem. System testing is concerned with control flow, recovery procedures, throughput, capacity and performance characteristics of the entire system. Bottom-up testing is easy to implement. This is because at the time of module testing, tested subordinate modules are available. The disadvantage, however is that testing of major decision / control points is deferred to a later period.
- ▶ **Top-down integration:** Top-down integration starts with the main routine, and stubs are substituted, for the modules directly subordinate

to the main module. An incomplete portion of a program code that is put under a function in order to allow the function and the program to be compiled and tested, is referred to as a stub. A stub does not go in to the details of implementing details of the function or the program being executed.

Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested with stubs. This process continues till the atomic modules are reached. Since decision- making processes are likely to occur in the higher levels of program hierarchy, the top-down strategy emphasizes on major control decision points encountered in the earlier stages of a process and detects any error in these processes. The difficulty arises in the top-down method, because the high-level modules are tested, not with real outputs from subordinate modules, but from stubs.

- ▶ **Regression tests:** Each time a new module is added as part of integration testing, the software changes. New data flow paths are established, new I/O may occur and new control logic is invoked. These changes may cause problems with functions that previously worked flawlessly. In the context of the integration testing, the regression tests ensure that changes or corrections have not introduced new errors. The data used for the regression tests should be the same as the data used in the original test.

System testing

System testing is a process in which software and other system elements are tested as a whole. System testing begins either when the software as a whole is operational or when the well defined subsets of the software's functionality have been implemented. The test target in this case is the whole implementation model for the system. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non- production test environment. The following types of testing might be carried out.

- i. **Recovery Testing:** Checking the ability of recovery of the system after the failure of hardware or software.
- ii. **Security Testing:** Ensuring the existence and proper execution of access controls in the new system.
- iii. **Stress or Volume Testing:** Testing the application with large quantity of data during peak hours to test its performance.
- iv. **Performance Testing:** Comparing the new system's performance with that of similar systems using well defined benchmarks.

Final Acceptance Testing

Final Acceptance testing is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and the system

Module 4, Chapter 2

satisfies the users. Thus the final acceptance testing has two major parts:

- i) **Quality Assurance Testing:** ensures that the new systems satisfies the prescribed quality standards and the development process is as per the organisation's quality assurance methodology.
- ii) **User Acceptance Testing:** ensures that the functional aspects expected by the users has been well addressed in the new system. There are two types of the user acceptance testing.
 - ▼ **Alpha Testing:** is the first stage, often performed by the users within the organization
 - ▼ **Beta Testing:** is the second stage, generally performed by the external users. This is the last stage of testing, and normally involves sending the product outside the development environment for real world exposure.

Implementation of Software

Planning of the implementation should be commenced much before actual date of the implementation and the implementation plan as developed in the Design Phase should be used with the modifications if required. While implementing the new system, if test data was used for carrying out testing, care should be taken to delete the same before making the new system live.

There are four types of implementation strategies:

Direct implementation / Abrupt change-over

In this strategy, the old system is suspended on a specific day and the new system is tried out. This is not recommended, because in case the new system crashes, the old system is also not available. In case of small applications, or when migrating from a manual to computer system, this may be used.

Parallel implementation

Both the old and new systems are run in parallel to verify if their output is the same. Then the old system is suspended.

Phased implementation

This strategy consists of implementing the new system in parts. This makes implementation more manageable.

Pilot implementation

The new systems is first implemented in a small, non-critical unit and then moved to larger unit.

Except direct implementation, others strategies are not mutually exclusive. A judicious combination of the strategies can be adopted, depending on the type of application.

Activities during Implementation Stage

Major activities during implementation are:

- ▶ Installation of new hardware / software
 - ▼ If the new system interfaces with the other systems or is distributed across multiple software platforms, some final commissioning tests of the production environment may be desirable to prove end to end connectivity.
- ▶ Data conversion: Following steps are necessary.
 - ▼ Determining what data can be converted through software and what data manually.
 - ▼ Performing data cleansing before data conversion
 - ▼ Identifying the methods to access the accuracy of conversion like record counts and control totals
 - ▼ Designing exception reports showing the data which could not be converted through software.
 - ▼ Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner
 - ▼ Actual conversion
- ▶ User Final Acceptance testing
 - ▼ Ideally, the user acceptance test should be performed in a secured testing environment where both source and executable codes are protected. This helps to ensure that unauthorized or last minute change to the system does not take place without going through the standard system maintenance process.
- ▶ User training
 - ▼ Manager's training on overview and MIS
 - ▼ Operational user training on how to use the software, enter the data, generate the output
 - ▼ EDP training on the technical aspects

Post Implementation Review

After the system stabilizes, a check should be done to ensure that the system has fulfilled the objectives. Otherwise, move back to the appropriate stage of the development cycle. The post implementation review should be performed jointly by the project development team and the appropriate end users or alternatively, an independent group not associated with the development process, either internal or external, should carry out the audit, to meet the following objectives:

1. Assess the adequacy of the system:
 - a. Whether the system met management's objectives and user requirements
 - b. Whether the access controls have been adequately implemented and actually working

Module 4, Chapter 2

2. Evaluation and comparison of the actual Cost Benefit or ROI as against the same projected in the feasibility study phase.
3. Recommend on the system's inadequacies and deficiencies
5. Develop a plan for implementing the accepted recommendations
6. Evaluate the system development project process

Maintenance is also part of the post implementation review. It can be categorized into four types:

Corrective maintenance

Correcting errors that may surface during the running of the application.

Adaptive maintenance

Rapid changes in technology may cause an application to be run in a new technical environment in the user site. This may require modifications to be made, and is known as adaptive maintenance. Web enabling a legacy application would fall in this category.

Perfective maintenance

Perfective maintenance is required when the user wants additional functionalities. Extending the purchase order system to cover service orders will fall in this category.

Preventive maintenance

When the software is changed to suit future maintainability, it is called preventive maintenance.

Umbrella Activities

In addition to the activities associated with each phase, there are many others which are undertaken throughout the life cycle; these are referred to as umbrella activities. Some of these activities are:

- ▶ Project tracking and control
 - ▼ Budgeting
 - ▼ Reporting
 - ▼ Review
 - ▼ Signoffs
- ▶ Quality assurance
- ▶ Configuration management
- ▶ Documentation
- ▶ Change management
- ▶ Reusability management
- ▶ Measurement
- ▶ Risk management

Summary

The design phase details how the proposed system will translate into a working model.

The steps involved in this phase are: Architectural design; Design of data / Information Flow; Design of database; Design of user interface; Physical design; and Selection of appropriate hardware and software.

The next phase is program construction. This phase actually converts the design into a working program. This phase ensures that the program is accurate, reliable, robust, efficient, readable, user friendly, and maintainable. The phase involves coding through the operations of programmers and system analysts. The coding follows debugging exercise.

The next phase is software testing. This is a process of testing software in a controlled manner to ensure it meets the specifications.

Software testing comprises of

- ▶ Unit testing
- ▶ Integration / Interface testing
- ▶ System testing
- ▶ Final acceptance testing

After the information system is through with the testing process, it moves on to the implementation phase. This involves installation of the new hardware and software, data conversion, user acceptance of the new system, user training and test runs.

The final stage of SDLC is the post implementation review phase, which involves assessment, evaluation, deficiencies, recommendations and corrective, adaptive, perfective and preventive maintenance.

In addition to the activities associated with each phase, there are others, which are undertaken throughout the life cycle, which are referred to as umbrella activities. Some of them are:

- ▶ Project tracking and control
- ▶ Quality assurance
- ▶ Configuration management
- ▶ Documentation
- ▶ Change management
- ▶ Reusability management Measurement
- ▶ Risk management



3 Alternative Methodologies of Software Development

✂ Learning Goals ✂

To provide an understanding of:

- ▶ Different approaches to system development – advantages, problems encountered and selection criteria
- ▶ Different aspects involved in maintenance of information systems

Data Oriented Systems Development

Transaction processing is an integral part of many organizations involving both the data and the processing system. Data oriented system development is a method for representing software requirements by focusing on data structure and not data flow while processing. Systems that optimize data usage are classified as data-oriented systems. This approach considers data independently of the processing that transforms the data. Management Information Systems (MIS) and Data Warehousing applications fall in this category.

Object Oriented Systems Development

Object Oriented Systems Development (OOSD) uses the object-oriented methodology. In this method, the system is analyzed in terms of objects and classes and the relationship between objects and their interaction. Objects are defined as entities that have both data structure and behaviour. Conceptually, an object is something that has a fixed or defined set of properties. For example if an employee record is an object, then the properties are employee name, employee ID etc.

In the object oriented approach, it is easier to establish relationships between any two entities of a program, whether it is a database or an application program, where each entity is considered as an object. In this way, two similar objects can be associated easily. It allows inheritance of properties from one object to create another, which simplifies the process of creating newer objects with all attributes as the older one, and some additional attributes. E.g. The principles of compound interest can be inherited from simple interest.

Major advantages of this approach are:

- ▶ Ability to manage a variety of data types
- ▶ Ability to manage complex relationships
- ▶ Capacity to meet demands of a changing environment

Module 4, Chapter 3

- Reusability of logical elements
- Data Security

Object Oriented technology is widely used in:

- Computer Aided Engineering (CAE)
- Systems software

This approach is gaining popularity in application development as well.

Prototyping

When a customer defines a set of general objectives for the software, but not detailed input, processing and output requirements, prototyping may be the best approach.

The following are the steps in the prototyping approach:

- Requirements gathering: The developer gets the initial requirements from the users.
- Quick design: The emphasis is on visible aspects such as input screens and output reports.
- Construction of prototype: by the developer on the basis of inputs from the users.
- Users evaluation of prototype: The users accepts the screens and options as shown to them.
- Refinement of prototype: Prototype is refined by fine tuning the users requirements.

The last two steps are iterated till the user is fully satisfied with the prototype.

The drawbacks of the prototyping approach are:

- The user sees the 'working' version of the software, without realising that the process engine is still not ready. So he starts making unreasonable delivery date demands without realizing the fact that prototype has to be expanded to handle transaction volume, client server network connectivity, backup and recovery procedures and the control features.

As the development has to be carried out very fast, the developer uses the 4GLs tools. But in the larger developments, design strategy has to be clearly laid down, otherwise the effort will result in poor quality, poor maintainability and low user acceptance resulting in the failure of the effort.

- The prototype is only for eliciting user requirements. Even the input and output programs may have to be rewritten taking into account the target environment and efficiency considerations. Having worked hard at developing a prototype, the developer tries to work around it to develop the application, thereby leading to sub optimality.

- ▶ The capability of the prototype to accommodate changes could also lead to some problems. The user may at times add changes at the cost of strategic objectives of the application.
- ▶ In prototyping, the software being developed is modified and coded, as and when the user feels the need for change. Hence, it becomes difficult to keep track of changes in the controls.
- ▶ Changes in design and development keep happening so quickly in this approach that formal change control procedures may be violated.

Though the IS auditor should be aware about the above risks associated with prototyping, the IS auditor should also be aware that this method of system development can provide the organization with substantial saving in time and cost.

Rapid Application Development (RAD)

RAD is an incremental model which has a short development cycle. But requirements have to be clearly understood and the scope has to be well defined. RAD leverages the following techniques to keep the development cycle short:

- ▶ Multiple small teams
- ▶ Modular applications
- ▶ Evolutionary prototype
- ▶ Automated tools
- ▶ Design workshops
- ▶ Component- based development
- ▶ Fourth generation languages
- ▶ Rigid time frames

The four stages in this approach are:

- ▶ Definition of scope
- ▶ Creation of a functional design
- ▶ Construction of application
- ▶ Deployment

The drawbacks of RAD are:

- ▶ For large projects, it requires a lot of human resources creating management problems.
- ▶ It is a joint effort between the customer and developer. If the commitment weakens on either side, the approach will fail.
- ▶ It is not suitable for monolithic applications.
- ▶ For mission critical applications, where quality and reliability assume higher importance than time of development, this approach is not recommended.

Reengineering

Many large organisations have a large number of applications that were developed 15 - 20 years ago. These programs have undergone many modifications over a period of time. These applications were developed at a time when many of the structured techniques had not evolved. In many, these techniques could have been violated.

It is difficult to migrate these huge mission critical applications to new systems quickly. But at the same time old applications become increasingly difficult to maintain because of the outdated technology, lack of vendor support or knowledge of programming languages.

In such cases, the reengineering approach is suggested. This is quite like remodeling I rebuilding an old house.

Software reengineering consists of six activities:

- ▶ **Inventory analysis:** Every organisation should have an inventory of all applications that it uses. This should include details such as size, age, business criticality. Applications can be sorted on the basis of business criticality, age, current maintainability and other locally important criteria. Then applications for reengineering can be selected. This analysis should be done on a periodic basis because factors such as current maintainability can undergo significant changes.
- ▶ **Document restructuring:** In many legacy applications, documentation is sketchy, or may not exist at all. In a large application environment, documentation must be carefully planned, taking into account the resources available. Static applications can be left with current level of documentation. While for dynamic applications, the documentation is updated, as and when the program is being modified. For critical applications, the documentation may be reworked completely.
- ▶ **Reverse engineering:** This is the technique of drawing design specifications from the actual product by studying its source code. In software reverse engineering, the program is first analyzed and then design specifications are worked out. This process can be carried out in several ways:
 - i. Decomposing the object or executable code into source code and using it to analyse the program
 - ii. Utilizing the reverse engineering application as a black box test and unveiling its functionality by using test data.

The advantages of the reverse engineering are faster development of a system and improvement in the present system by using reverse engineering. The IS auditor should be aware that many software

license agreements prohibit reverse engineering to safeguard their trade secret and programming techniques.

- ▶ **Code restructuring:** After source code analysis, a list is made of programs, which are difficult to maintain because of non-standard coding. These programs are restructured, tested and updated.
- ▶ **Data restructuring:** In this stage, the data files / database is reviewed and restructured. Since data architecture has a strong influence on program architecture, code level changes will follow data restructure.
- ▶ **Forward Engineering:** In this stage, the design decided upon in the reverse engineering stage is analyzed and perfected.

For many of these steps, automated tools are available for assistance.

Structured Analysis

Structured analysis is a framework for the physical components (data and process) of an application. It is based on data flow diagrams

The advantages of using this approach are as follows:

- ▶ It is an efficient and easy to understand documentation and communication tool between users and developers
- ▶ Automation is easy. CASE tool support is available.

The drawbacks of Structured analysis are:

- ▶ Time intervals between tasks are not represented. It does not offer inputs for designing concurrent tasks.
- ▶ Conditions and selection cannot be represented.

Web based Application Development

The World Wide Web and the Internet have drawn great importance into the world of computing. With the help of Web based Applications, we purchase shares, download music, view movies, get medical advice, book hotel rooms, schedule airline flights, do our banking, take college courses etc.

Web-based systems and applications become integrated in business strategies for small and large companies. The following are the attributes of the Web based applications.

1. **Network Intensive:** By its nature, a web based application is network intensive. It resides on a network and must serve the needs of diverse community of clients. A web based application may reside on the internet (thereby enabling open worldwide communication) or intranet (implementing communication across the organisation) or extranet (inter network communication).
2. **Content Driven:** In many cases, the primary function of a web based application is to use hypermedia to present text, graphics, audio, and video contents to the end user.

Module 4, Chapter 3

3. **Continuous evolution:** Unlike conventional application software that evolves over a series of planned, chronologically spaced releases, web based applications evolve continuously.

The following application categories are most commonly encountered in Web based applications.

- ▶ **Informational:** Read only content is provided with simple navigation and links
- ▶ **Download:** A user downloads information from the appropriate server
- ▶ **Customization:** The user customizes contents to specific needs
- ▶ **Interaction:** Communication among a community of users occurs via chat-room, bulletin boards, or instant messaging.
- ▶ **User Input:** Forms based input is the primary mechanism for communicating need
- ▶ **Transaction oriented:** The user makes a request (e.g. places an order) that is fulfilled by the web based application
- ▶ **Service Oriented:** The application provides a service to the user (e.g. assists the user in calculating the EMI of loan)
- ▶ **Portal:** The application channels the user to other web content or services outside the domain of the portal application
- ▶ **Database Access:** The user queries a large database and extracts information
- ▶ **Data Warehousing:** The user queries a collection of large databases and extracts information

The web based application development process begins with formulation – the activity that identifies the goals and objectives of such development, planning estimates of overall project cost, evaluates risks associated with the development effort, and defines a development schedule. Analysis establishes technical requirements for the application and identifies the content items that will be incorporated. The engineering activity incorporates two parallel tasks: content design and technical design. Page generation is a construction activity that makes heavy use of the automated tools for the web based application and testing ensures web application navigation, attempting to uncover errors in function and content, while ensuring that the web based application will operate correctly in the different environments. Web engineering makes use of an iterative, incremental process model because the development timetable for web based applications is very short.

In case of Web Based Applications, the clients database resides on a back end processor and the software and the data related to the frequently asked information may reside on a front end (unlike client server based applications where both may reside on the same processor) so as to save the time of the querist.

Risks associated with Web Based Applications:

1. As the Web based applications are available via network access, it is difficult to limit the possible end users who may access the application. In order to protect the sensitive content and provide secured modes of data transmission, strong security measures must be implemented throughout the infrastructure that supports a Web Based Application and within the application itself.
2. In the absence of disciplined process for developing Web Based Systems, there is increasing concern that we may face serious problems in the successful development, deployment and maintenance of these systems. Poorly developed Web Based Applications have too high probability of failure. As Web Based Systems grow more complex, a failure in one can and will propagate broad based problems across many. In order to avoid this, there is pressing need for disciplined Web engineering approaches and new methods for development, deployment and evaluation of Web based systems and applications.

Agile Development

The term agile development refers to a family of similar development processes that involves a non traditional way of developing a complex system. One of the first agile process which emerged in 1990s was Scrum, which aimed to planning and directing tasks from the project manager to the team thus helping the project manager to remove the obstacles to the team to achieve their objectives. Thereafter, further agile processes, such as Extreme Programming (XP), Crystal, Adaptive Software Development, Feature Driven Development and Dynamic System Development Method have emerged.

These processes are termed as “agile” because they are designed with flexibility to handle changes to the system being developed or the project team that is performing the development.

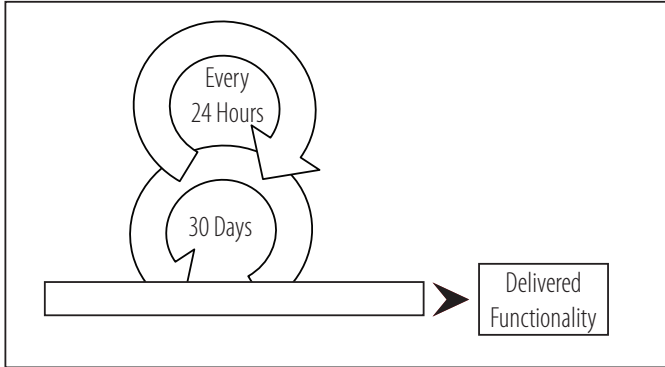
Agile development process involves:

1. Setting of small subprojects or iterations on the basis of which next iteration is planned.
2. Replanning the project at the end of each iteration involving resetting priorities, identification of new priorities etc
3. The teams are generally small, cohesive and comprise of both business and technical representatives.
4. In case of some agile development, two programmers code the same part of the system as a means of knowledge sharing and quality improvement.

Module 4, Chapter 3

5. Unlike a normal project manager has the role of planning the project, allocating the tasks and monitoring the progress of the project, the project manager has a job of facilitator and advocate.

Agile Development



Agile development does not ignore the concerns of traditional software development but approaches them from a different perspective.

1. Agile development plans for the next development in detail, rather than planning subsequent development phases far out of time.
2. Agile development's adaptive approach to requirements does not emphasize managing a baseline requirements.
3. Agile development's focus is to quickly prove an architecture by building actual functionality against development of formal more detailed models and descriptions.
4. Agile development assumes limits to detect testing but attempts to validate functions through a frequent build test cycle and to correct problems in the next subproject before too much time and cost is incurred.
5. Agile development does not emphasize defined and repeatable process, but instead performs and adapts its development based on frequent inspections.

Information Systems Maintenance Practices

After a system is moved into production, it seldom remains static. Change is a reality, and systems undergo changes right through their life cycle. These changes often create problems in the functionality and other characteristics of a system. So it is necessary that a procedure for change is formalized.

Change control

Any request for change by the user has to be submitted to the EDP department, along with the reasons for change. (In case the developer

himself wants to change the program to overcome a processing problem or improve performance, then he has to prepare a written change request document).

The user request is then assessed by the relevant application developer. He evaluates the impact of the modifications on other programs. The number of days required to make all the necessary changes, time for testing and changes in documentation is also estimated. A report is then prepared by the developer on the basis of time and cost of change.

Every organisation should have a defined Change Control Authority (CCA) – a person or a committee – which is the final authority to approve changes. The CCA will review the report and approve/reject the change request. An Engineering Change Order (ECO) is then generated for the changes approved.

The ECO describes the change that should be made; constraints within which change should be made; and criteria for review and audit. The program(s) to be changed is / are then copied to the test directory from the production directory with access control for the designated programmer.

The programmer then makes the approved changes, and the programs go through all the tests that they had gone through, when they were initially developed. If a program change warrants a change in the database, then it is first made in the in the test data base, and all related documents are changed.

The CCA then reviews the changes made to programs, data and documents. Then after it is approved, the systems administrator moves the changed version into the production directory, and informs all users of the change and the revised version number.

After running the new version of the application the user who requested the change should certify that the change requested by him has been fulfilled.

Maintenance records of all programs should exist in hard copy form or in the machine. The maintenance records should include the programmer id, time and date of change, change request number, and before and after images of program lines, which were changed. Library management software available, which help controlling the changes on the machine are available.

Automated change control software is useful in preventing unauthorised program changes. This is particularly necessary if the role of the systems administrator has not been well defined and programmers themselves run the application. The change control software will then

Module 4, Chapter 3

be responsible for migrating changed programs to the production directory and not operations personnel.

Continuous update of systems documentation

To effectively maintain systems, documents should reflect the current version of the software. Often time and other resource constraints, as well as tedious procedures the result in programs not being updated. Documents that have to be kept updated are:

- ▶ System manual
 - ▼ Input screens
 - ▼ Output reports
 - ▼ Program specifications
 - ▼ Flow charts, Decision tables, Decisions trees
 - ▼ Narrative of program logic
 - ▼ Data dictionary
 - ▼ Entity relationship diagram
 - ▼ Object diagrams
 - ▼ Data flow diagrams
- ▶ User manual
 - ▼ Data entry procedures
 - ▼ Batch operation procedures

The current version of the documentation should also be available on the back-up site.

Program migration process

During change control, the process of taking out one or more copies of program(s) from the production directory and moving them back to the production directory are important steps that require additional control.

These are also referred to as 'check out' and 'check in'. Only an authorised software engineer can check out the program(s). This is controlled by the access control software. The systems administrator copies the program(s) to the test directory and controls the access to a particular user-id and password, which he discloses only to the authorised software engineer. Similarly after the changes are made, it is the responsibility of the systems administrator to copy the changed version into the production directory. Then access for the specified user ID and password are disabled.

In the change control process, Synchronization Control stops parallel changes from being made by two different programmers. Once a program is checked out for change, Synchronization Control locks it against release for any other change. Only after the program is checked in, is it unlocked

Testing program changes

While assessing the effectiveness of the change control procedure, the auditor should check if:

- ▶ All change requests are documented in a standard form containing
 - ▼ Adequate description of change desired
 - ▼ Explanation of reasons for change request
 - ▼ Signature of the requestor
 - ▼ Date of request
- ▶ Cost and time analysis of change has been conducted by the developer.
- ▶ It is compliant with the approval process for change request
- ▶ Access rights and the rationale behind them have been clearly defined
- ▶ The process of checking in and communicating change to the users is being implemented.
- ▶ The configuration audit process is done (a periodic review of the changes made to configuration items)

If the auditor so desires, he can take a change request and trace all activities from the documentation to assure himself that all the processes are being followed.

Library control software

The purpose of the library control software is to separate production libraries from test libraries.

The following are the functions of this software:

- ▶ It prevents programmers from accessing source and object programs in the production directory.
- ▶ It does not permit program to be updated in bulk.
- ▶ It enforces discipline: The programmer after making the requested change in the source code and testing it hands it over to the official authorised by the organisation to update the production directory - control group or systems administrator. The production directory is then updated with the revised version of the code - source and object.
- ▶ It provides read-only access to the source code. Any modification has to be authorized by the change control procedure detailed earlier.
- ▶ It maintains clear distinction between programs in production and test directories.

Executable and source code integrity

At any point of time, the current version of the source code and object code should match. In a manual program migration practice, the changed source code may be moved to the production directory, but compilation is omitted. In such a case, the previous version of object code continues executing. Thus, when the auditor checks the source

Module 4, Chapter 3

code, it does not correspond to the object program. To overcome this difficulty Library Control Software is employed to automate the process of conversion. Once the source code is moved to the production directory, the software takes the responsibility of converting it to the object code.

Some of the controls the auditor should use to check in code integrity are:

- ▶ The time stamp on the object code should always be later than that of the corresponding source code.
- ▶ Users and application programmers should not have access to the production source code.

In an automated environment, where the users themselves develop applications, controls may be lax. So auditors should focus on evaluating controls in such applications

Program code comparison

Auditors use program code comparison to ensure that the source code provided to them for review is the same as the one that has been compiled to produce the current version of object code.

Program code comparison can be of two types:

- ▶ Source code comparison
- ▶ Object code comparison

Source code comparison

The IS auditor should check whether the current / latest version of the source code and the version that is available in production directory are the same. Software to check this is now available.

While manual checking is feasible in source code comparison, it may not be effective: In languages like Cobol, even column number will matter in the functioning of the program. In languages such as C, a punctuation mark can make a difference. Almost all languages permit comment lines with a prefix of asterisks. So lines of code that are prefixed with asterisks will be physically present but not functional. So if an auditor is attempting a manual check, he should be very thorough, taking care to verify the column number and punctuation.

While using software for code comparison, the auditor should know to differentiate material and non-material changes between the codes. For example, change of position of text does not make any difference in many languages. But the software mechanically will report this as a difference between the codes. The auditor however should recognise that this change will not materially affect the functioning of the program.

Object code comparison

Object code comparison is more difficult, because the object code is not readable. This is done through following steps:

- ▶ After going through the source code comparison, the auditor should compile a copy of the source code in the production directory and generate an object code.
- ▶ The test plan for the program should be applied on the object code and the results must be documented.
- ▶ The same test data has to be applied on the object code available in the production directory.
- ▶ The results of both these tests should match.

Emergency changes

Sometimes emergency changes may have to be made. If the management recognises that there is not much time available to create a new version because of an extraordinary situation, they can relax the change control procedure. Normally, this is operated by a special log-in id, which is known only to systems administrator and may be available in a sealed envelope with the EDP management. With the approval of the management, the programmer may access the production directory using the special log-in ID and make the necessary changes in the program and run the new version to create outputs. These must be diligently logged in the machine. The follow-up procedure will include all necessary documentation and written approvals post-facto.

Configuration Management

Configuration management involves various procedures throughout the life cycle of the software to identify, define and baseline software items in the system thus providing a basis for problem management, change management and release management.

Configuration management process involves identification of items like programs, documentation and data. Configuration management team can be formed to whom the programs, documentation and data as stated above is handed over for safekeeping. Each is assigned a reference number for a quick retrieval. Once handed over to the configuration management team, the item cannot be changed without a formal change control process which is approved by a change control group.

The process of moving an item to the controlled environment is called checking in. When a change is required, the item will be checked out by the configuration manager. Once the change is made, it is checked in by a different version number.

Module 4, Chapter 3

To make configuration management successful, management's support is very much required. The job profile of the maintainer involves the following task steps:

1. Develop the configuration management plan
2. Baseline the code and associated documents
3. Analyse and report on the results of configuration control
4. Develop the reports that provide configuration status information
5. Develop release procedures
6. Perform configuration control activities, such as identification and recording of the request
7. Update the configuration status accounting database

Program Evaluation Review Technique (PERT) and Critical Path Method (CPM) are the techniques used to monitor the project in such detailed level. These are dealt with in the next chapter.

Summary

A few of the alternate approaches to system development are: Data-oriented approach, object oriented design, prototyping, RAD (Rapid Application Development), Reengineering and Structure Analysis. In the object-oriented analysis, the system is analyzed in terms of objects and classes and the relationship between objects and their interaction. Object Oriented Technology is widely used in Computer Aided Engineering (CAE) and systems software. In prototyping a set of general objectives for the software is defined, instead of listing detail input/output and processing requirements. RAD is an incremental model that supports a short development cycle. In this approach, the requirements must be clear and the scope must be well-defined. Reverse engineering or reengineering involves separating the components of a system and observe its working with an intention of creating its replica or improving upon the original product. Structured analysis is a framework for the physical components (data and process) of an application. It is done using data flow diagrams. Web based applications development deals with such application systems which work on the networks to make available the information to the users. Agile development involves similar development processes that involves a non traditional way of developing a complex system.

Once a system is moved into production, it seldom remains static. The changes in the system often create problems in the functionality. So it is necessary that a systematic approach to maintain the information system is formulated and implemented. These processes collectively are referred to as information systems maintenance practices. They include

change control, continuous updating of systems documentation, program migration process and testing.



4 Project Management Tools and Techniques

✂ Learning Goals ✂

To provide a clear understanding of:

- ▶ The significance of budgets and schedules in system development
- ▶ PERT (Program Evaluation Review Technique) as a project management tool, including:
 - ▼ Events and activities in a project
 - ▼ Data sheet
 - ▼ Time Estimate
- ▶ Various kinds of CASE tools and techniques available for project management, including:
 - ▼ Code generators
 - ▼ Critical Path Method (CPM)
 - ▼ Computer Aided Software Engineering (CASE) and its tools
- ▶ The role of an auditor in a CASE environment.

Introduction

There are many tools available for a Project Manager to plan, control and monitor activities in a project. The most appropriate tool or technique should be chosen, depending on the size and complexity of the project.

Budgets and schedules

Two critical problems in software development are: Time and cost overruns need to be addressed by a project manager. These problems arise because of poor estimation of effort required and hence cost involved in developing an application.

A continuous effort has been made to refine the effort estimation procedure. Many organisations use the function point approach to arrive at this estimate. A function point represents the size and complexity of the application and this is computed on the basis of number of inputs, outputs, files, queries and interfaces that the application is likely to have. This estimate is arrived at in terms of person-months required to develop the application.

Now this gross person-month effort has to consider details, such as:

- ▶ What are the activities in the project?

Module 4, Chapter 4

- ▶ In which sequence will these activities be performed?
- ▶ How will the total person-month effort be distributed over these activities, i.e. how much time will each activity take and how many persons of which type of skills will be required for each of these activities?
- ▶ On which date will each activity start and finish?
- ▶ What additional resources are required to complete the activity?
- ▶ What will be the measure that assesses the completion of an activity?
- ▶ What will be the points in which the management will review the project? (In Project Management terminology, these are referred to as milestones.)

Software Cost Estimation

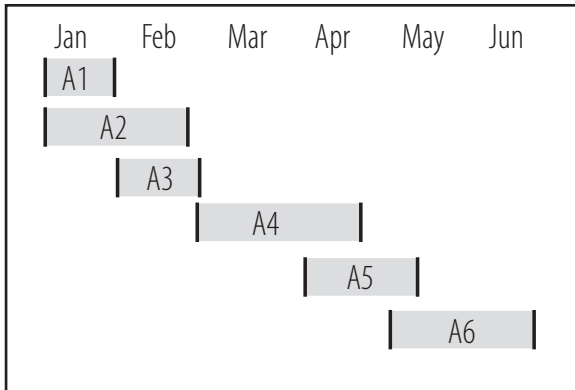
Automated techniques at each phase of system development are available for cost estimation. To use these products, a system is divided into the main components and a set of cost drivers is established.

Components include:

1. Main storage constraints
2. Data storage constraints
3. Execution Time constraints
4. Staff experience
5. Computer access
6. Security environment
7. Source code language
8. Target machine used for development

Gantt Charts

Gantt Charts are prepared to schedule the tasks involved in the software development. They show when the tasks should begin and end, what tasks can be undertaken concurrently, and what tasks must proceed serially. They help to identify the consequences of early and late completion of the tasks. The following is a sample Gantt Chart:



In the above Gantt Chart,

1. Activity A1, A3, A 4 are the serial activities which meaning A3 succeeds A1 and A4 succeeds A3 while,
2. Activities A1 and A2 are activities with concurrent beginning, while
3. Activities (A2, A3) and (A4, A5 and A6) are the overlapping activities with different beginning and end dates.

Program Evaluation Review Technique (PERT)

PERT represents activities in a project as a network. It indicates the sequential and parallel relationship between activities.

PERT terminology

Activity

An activity is a portion of the project, which requires resources and time to complete. The activity is represented by an arrow. The following diagram, shows activity A to activity H.

Event

An event is the starting or end point of an activity. It does not consume resources or time. It is represented by the starting circle in the following diagram.

Predecessor activity

Activities that must be completed before another activity can begin are called predecessor activities for that activity. In the following figure, Activity A is the Predecessor Activity for Activity E

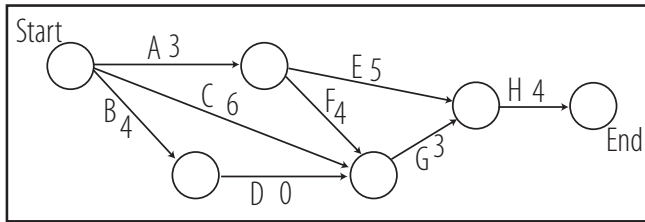
Successor activity

Activities that are carried out after an activity is completed are known as successor activities. In the following figure, Activity E is the successor activity of Activity A while Activity G is the successor activity for Activities F, C and D

Module 4, Chapter 4

Slack

Slack is the difference between earliest and latest completion time of an activity.



Maximum Total duration of this project = 14 days

While the earliest B can start on the 0th day, the project duration will not be affected even if it is started after one day. So the latest start day for D is 1. Hence Slack = $1 - 0 = 1$. Similarly, for D, earliest start day = 4, latest start day = 5 and slack is 1.

Dummy

Dummy activity is that activity which requires no resources. In the above figure, activity D is the dummy activity. A dummy activity does not have any real life significance. Dummy activities are required in PERT, because as per the rules of PERT, not more than one activity can have the same preceding and succeeding activity. To represent this, dummy activities are included.

Time estimate

PERT recognizes the estimates cannot be precise, and hence allows a weighted average of different estimates such as pessimistic, optimistic and most likely. A heavier weightage is given to the most likely estimate and the calculation is as follows:

to - optimistic estimate

tp - pessimistic estimate

tm - most likely estimate

Expected time = $(to + 4tm + tp) / 6$

Critical Path Method (CPM)

In a network, critical path represents the path which has the highest duration of time. For example, in the PERT network shown above, the following are the various paths from Start to End with their durations

Path 1: A - E - H = 12 days

Path 2: A - F - G - H = 14 days

Path 3: C - G - H = 13 days

Path 4: B – D – G – H = 11 days

Critical Path is Path 2 which has highest duration of 14 days. The importance Critical path assumes importance in Project Management, because it is the shortest time in which the project can be completed. Maximum control is required on the completion of any activity on Critical Path because if any activity on this path gets delayed, the whole project will be delayed.

Activities in the critical path have zero slack.

The critical path is found by working forward through the network, computing the earliest possible completion time for each activity, and thus earliest possible completion time for the project is found. Now taking this as the completion time of the project, working backwards the latest completion time of each activity is found. The path on which activities have the same earliest and latest completion time is the critical path or in other words slack is zero.

For effective monitoring of the project, activities in the critical path have to be closely monitored. When there is contention for a resource between activities, critical path activities should be given preference. If the duration of the project has to be reduced, then it should be seen how activities in the critical path can be crashed - meaning how their duration can be reduced.

System Development Tools and Productivity Aids

Code generators

Code generators generate program code on the basis of parameters defined by system analyst or data flow diagrams. These aid in improving programmer efficiency. Such tools, which help in automation of software life cycle activities are included in CASE (Computer Aided Software Engineering) tools.

Computer Aided Software Engineering (CASE)

CASE is an attempt to automate all activities associated with the software development life cycle.

The functionality some of the CASE tools is described below:

Project planning tools

There are two sets of tools available under this category:

- ▶ Estimation tools
- ▶ Scheduling tools

Estimation tools help in computing effort estimation and consequently duration and manpower requirement for the project.

Module 4, Chapter 4

Scheduling tools enable definition of tasks and creation of task network. Tools that help generate work breakdown structure and PERT diagram fall into this category.

Risk analysis tools

Risk analysis tools help to build a risk table by providing guidelines to identify and analyse risks

Requirement tracing tools

The objective of the requirement-tracing tool is to isolate customer requirements. This is done by parsing the RFP or users' specification through an interactive text evaluation. Then the parsed requirements are stored in a database.

Analysis and design tools

These help in creation of system models - data flow and ER diagrams.

Process modelling tools

There are a variety of prototyping tools. Screen painters help to define a screen layout rapidly for interactive applications. More sophisticated tools enable creation of data design with screen and report layouts. Many of the fourth-generation languages have prototyping features.

Web application development tools

These help in generating components of a web page such as text, graphics, forms, scripts and applets.

Quality assurance tools

These tools help to comply with standards.

Testing tools

There are different categories of testing tools:

- ▶ **Static analysis tools:** The static analysis tool graphs programs and analyses their quality based on those graphs to produce several standard types of source language metric summary level analysis, including analysis of code complexity, structure and defects
- ▶ **Code-based testing tools:** These accept source code as input and perform a number of analyses that result in generation of test cases.
- ▶ **Specialised testing languages:** These enable software engineers to write detailed test specifications that describe each test case and logistics of its execution.
- ▶ **Requirements-based Testing Tools:** These isolate user requirements and suggest test cases that test these requirements

Dynamic analysis tools

These tools check the flow of the program.

Documentation tools

These tools aid in the production of documents associated with all life cycle activities.

Metrics tools

These tools capture metrics such as LOC / person month, defects / function point and the like.

Configuration management tools

This tool provides a database for storing information about different versions of configuration items. Change control procedures can also be implemented with these tools. Well-defined categorized storage of configuration items aids the audit process also.

Reengineering tools

The following types of tools fall under this category:

- ▶ Reverse engineering tools: These take source code as input and generate graphical analysis and design models.
- ▶ Code restructuring tools: These analyse program syntax, generate control flow diagram and structure the program.
- ▶ Data restructuring tool: These help in generating entity-relationship diagram from the database.

Classification of CASE tools

CASE tools are generally divided into three categories, depending on the stage of the life cycle at which they can be used.

- ▶ **Upper CASE:** These tools are useful in the early stages of system life cycle. Tools that help in defining application requirements fall in this category.
- ▶ **Middle CASE:** These tools address the needs in the middle levels of SDLC such as Design. Those that help in designing screen and report layouts, data and process design falls in this category.
- ▶ **Lower CASE:** The later parts of the life cycle make use of these tools. These tools use design information to generate program codes.

Integrated CASE environments

While it is possible to use separate CASE tools for individual activities, an integrated CASE (I CASE) tool can be used for better efficiency.

CASE database

A CASE database or repository, as it is called, in an integrated CASE environment will contain the following data:

- ▶ Enterprise information
 - ▼ Organisational structure
 - ▼ Business area analysis
 - ▼ Information architecture

Module 4, Chapter 4

- ▶ Application design
 - ▼ Model diagrams
 - ▼ Naming standards
 - ▼ Referential integrity rules
 - ▼ Entity / object definitions
 - ▼ Data structures
 - ▼ Process definitions
 - ▼ Menu trees
 - ▼ Performance criteria
 - ▼ Screen definitions
 - ▼ Report definitions
 - ▼ Processing logic
- ▶ Construction
 - ▼ Source code
 - ▼ Object code
 - ▼ Change information
- ▶ Testing
 - ▼ Test plan
 - ▼ Test results
 - ▼ Quality metrics
- ▶ Project management
 - ▼ Project plan
 - ▼ Work breakdown structure
 - ▼ Estimates, schedules
 - ▼ Problem reports
 - ▼ Change requests, status reports
 - ▼ Audit information
- ▶ Documentation
 - ▼ Systems requirements specifications
 - ▼ Design document
 - ▼ User manuals

Advantages and limitations in using CASE

Benefits of using CASE

- ▶ Since CASE strictly follows SDLC, use of CASE enforces the discipline of following steps of SDLC .
- ▶ The standardization / uniformity of processes can be achieved.
- ▶ Since CASE tools generate inputs of each stage from the outputs of previous stage, consistency of application quality can be ensured.
- ▶ Tasks such as diagramming, which are monotonous, need not be done by the programmer, and can be left to the CASE tool.

- ▶ This results in deploying the programmer for more productive tasks; thus the development time can be shortened and cost economy can be achieved
- ▶ Since stage outputs and related documentation are created by the tool.

Disadvantages of CASE

- ▶ CASE tools are costly, particularly ones that address the early stages of the life cycle.
- ▶ Use of CASE tools requires extensive training

Auditing CASE environment

The auditor should be aware of the changes between the application development process in non-CASE and CASE environments. Since CASE introduces many disciplines and enforces standards and consistency, many of the tasks of auditor might become easier. However, the auditor should address the following issues:

- ▶ In case different tools are used at different stages, then the interface between these tools should be checked to make transition easy and ensure consistency.
- ▶ The integrity of data between manual process and CASE tool and vice-versa should also be checked.
- ▶ The appropriateness of the tool to the application development methodology should also be checked
- ▶ The auditor should check the manner in which changes are introduced at different stages of the development process. They must be the consistent throughout the stages.
- ▶ CASE does not automatically guarantee application controls. The auditor should check this aspect, as he would do in a traditional application development environment
- ▶ The CASE data base security and access controls should also be checked.

 Summary

The two important issues to be addressed by a project manager in the process of software development are time and cost overruns. As estimates are not very accurate, more time and money is required to complete a project

A continuous effort to refine the effort estimation procedures has resulted in the development of many system development and project management tools. These enable the developer to represent the size and complexity of the application and evaluate the project cost / time estimate on the basis of number of inputs, outputs, files, queries and interfaces that the application is likely to have.

Module 4, Chapter 4

The widely used approaches are Gantt Chart, Program Evaluation review Technique (PERT) and Critical Path Method. These approaches are used to relate the activities in a project.

Gantt Chart shows when the tasks should begin and end, what tasks can be undertaken concurrently, and what tasks must proceed serially.

PERT is able to represent the sequential and parallel relationship between activities. It realises that estimates cannot be spot on, and hence allows a weighted average of different estimates such as pessimistic, optimistic and most likely. A heavier weightage is given to the most likely estimate.

Another widely used approach in estimating time in the process of system development is Critical Path Method often referred to as CPM. In a network, the critical path represents the path, which has the highest duration of time among different paths. This assumes importance in project management, because it is the shortest time in which the project can be completed.

In an attempt to automate all activities associated with software development Computer

Aided Software Engineering was (CASE) was formulated. Some of the tools employed in CASE are project planning tools, prototyping tools, requirement tracing tools, web application development tools, testing tools, documentation tools and metric tools.

An auditor should be aware of the changes between the application development process in non-CASE and CASE environment. Since CASE enforces standards and consistency. It makes the auditor's job much earlier.



5 Auditing the System Development Process

✂ Learning Goals ✂

An understanding of the IS auditor's role in developing an information system

IS Auditor's Role in Systems Development, Acquisition and Maintenance

The different development models discussed earlier make us wonder how the IS auditor will check the compliance of systems. For each system, the auditor elicits the information about the methodology used for development and assesses its suitability for the system. This can be done by interviewing the project management team. After he is convinced about the suitability of the process, he can check the compliance of the process with the existing system. This process generally includes the following:

- ▶ Identifying subsystems and modules, their goals and user functionality expectations. The auditor does not undertake this task of identification himself. He goes through the analyst's findings and cross-checks them. Identification of these details becomes necessary to suggest the required controls.
- ▶ Checking if the control recommendations are appropriate for the risks identified in the project. The auditor reviews the risk analysis done by the analyst, and verifies if all the risks have been covered through user interviews.
- ▶ Advising the design team on incorporating control measures. The user also needs to be convinced about the control measures that have to be in place, and this too is the auditor's responsibility.
- ▶ Verifying if the recommendations he has made are properly implemented. To achieve this objective, he has to monitor the design process.
- ▶ Apart from ensuring control aspects, the auditor also has to ensure that the systems help to meet the organisational objectives.
- ▶ Reviewing the system development methodology to ensure the quality of the deliverables. He has to check for adherence to stated methodology documentation and other deliverables.
- ▶ Reviewing the change management process and effectiveness of its implementation.

Module 4, Chapter 5

- ▶ In the post implementation phase, the delivery and project management team may cease to exist, so the auditor will have a greater role to play in assessing the effectiveness of the system.
- ▶ Reviewing the maintenance procedure and ensuring that adequate documentation has been maintained for related activities. Lax controls in this phase can also have an adverse effect on the systems, so the auditor should continue to monitor the maintenance procedures.
- ▶ Ensuring production source integrity during the maintenance phase.

IS Auditor's Role in Reviewing Developmental Phases of SDLC

The IS auditor also has to review all the phases of the system development life cycle, such as:

1. Feasibility study
2. System requirement definition
3. Software acquisition
4. Detailed design and programming
5. Testing
6. Implementation
7. Post-implementation and maintenance
8. System change procedures and program migration process

The responsibilities of the IS auditor in each of these phases is given below:

Feasibility study

While reviewing the feasibility study phase, the IS auditor has to consider the following questions:

- ▶ Has there been an agreement in the definition of the problem among all stakeholders?
- ▶ Was there a genuine need for solution established?
- ▶ Were alternate solutions considered? Or was the feasibility assessed on the basis of a single solution?
- ▶ What was the basis for the choosing the solution?

What is the extent of the problem perceived and how extensive is the impact of the solution likely to be? These give valuable inputs for evaluating feasibility.

Feasibility is incomplete without establishing clearly, the requirement and the technology proposed. In other words, the auditor has to ensure that the suggested technology is viable before implementing it in the development process.

In cost-benefit analysis, there could be a tendency to understate costs and overstate benefits. There could also be inaccuracies in identification and quantification of benefits. The auditor can provide a valuable inputs in evaluating the cost-benefit analysis.

Requirement definition

- ▶ The auditor should collect a copy of Systems Requirement Specifications (SRS) document and review it in terms of:
 - ▼ Problem definition
 - ▼ Information flows
- ▶ The auditor can also evaluate the methodology employed and the compliance level.
- ▶ The auditor should also check whether CASE tools were used, because the quality of work is likely to be better in CASE environments.

Software acquisition process

- ▶ The decision to acquire the software should flow from the feasibility study. The auditor should ensure that it is so.
- ▶ The auditor should also ensure that the software acquired would meet the overall design goals of the proposed system, identified during requirement analysis phase.
- ▶ RFP (Request for proposal) should be checked for adequacy. Details such as transaction volume, data base size, turn around time and response time requirements and vendor responsibilities should clearly be specified in RFP
- ▶ The auditor should also check the criteria for pre-qualification of vendors.
- ▶ Similarly, there should be sufficient documentation available to justify the selection of the final vendor / product.
- ▶ The auditor may also collect information through his own sources on vendor viability, support infrastructure, service record and the like.
- ▶ The auditor should thoroughly review the contract signed with the vendor for adequacy of safeguards and completeness. The contract should address the contingency plan in case of vendor failures such as, source code availability and third party maintenance support He should also ensure that the contract went through legal scrutiny before it was signed.

Detailed design and programming phases

- ▶ CASE environment simplify the tasks that have to be done by the IS auditor. This is because the CASE tools ensure quality and consistency of design, a major concern of auditors. In non-CASE environments, the auditor may have to undertake a detailed design review:
- ▶ The design diagrams should be checked for compliance with standards

Module 4, Chapter 5

- Any change that has been incorporated in the design stage should have appropriate approvals and this should be checked.
- The auditor should check the design for modularity.
- The auditor should review the input, processing and output controls of systems.
- Design of input screens and output reports is an area, in which auditors can offer valuable suggestions. The auditor should check the user interface design for usability, appropriateness, compliance with standards and acceptance by users.
- Audit trails are important the auditor should ensure its availability and adequacy in the design
- In the recommendation of hardware and software choices, the auditor should look for compatibility, interoperability and scalability conditions.
- Flow charts and other such tools should be checked for key calculations. Their implementation in programs also should be checked with the help of a programmer who is knowledgeable about the programming language.
- Exception data handling is an area that the auditor has to focus on. He has to test the design and program for such data.
- Unit test results should be reviewed. The auditor has to ensure that the 'bugs' have been fixed.

Testing phase

- The auditor should review the test plans for completeness.
- Cyclical processing such as month-end reports should be verified.
- Security functions of the system also have to be verified.

Implementation phase

- The documentation on parallel run, if available, should be reviewed for effectiveness.
- Operating procedures should be checked for clarity and accuracy,
- System and user documents should be checked for adequacy, clarity and currency.
- It should be ensured that data conversion has been completed and all past data are available in a format readable by the new software.

Post-implementation review

This review mainly addresses the issue of system's ability to fulfill objectives that were specified initially. Apart from this, the auditor has to check the following aspects:

- Compliance with change control procedure
- Functioning of controls in accordance with design
- Review of operator error logs

System change procedures and program migration process

On a periodic basis, the auditor should check the following:

- ▶ Procedures for authorising, prioritising and tracking system changes
- ▶ Appropriateness of authorisations for selected change requests
- ▶ Existence of program change history
- ▶ The match program and documentation versions
- ▶ Access control procedures on source and executable codes in production directory
- ▶ Procedure for emergency changes
- ▶ Security of emergency login ids.
- ▶ The match between current version of source code and executable code in production directory

IS Auditor's Role in Project Management

Apart from the phases of SDLC, project management is also subject to audit - particularly with respect to recognition and management of risks during different phases. The risk management process includes the measures undertaken to mitigate the risks at costs commensurate with the level of risks. Not recognising risks or providing exorbitantly costly mitigation measures for trivial risks should be avoided and this is the main focus of IS audit of project management activities.

To achieve the objective, the IS auditor can undertake the following activities:

- ▶ Collect documentation of each phase and check for adequacy and completion.
- ▶ Attend project meetings to check the compliance of the development process.
- ▶ Advise the team on adequate and cost effective control measures.
- ▶ Represent the management interest in the team by continuously assessing the ability of the team to meet targets that have been set.

Summary

An IS auditor gathers insights from the methodology used for development and assesses its suitability for the system. This can be also done by interviewing the project management team. Once the auditor is convinced about its suitability, he can check compliance with the stated process.

The reviewing process generally entails

- ▶ Identifying subsystems and modules, their goals and user functionality expectations
- ▶ Identifying and reviewing risks involved in the project
- ▶ Incorporating controls in the design

Module 4, Chapter 5

- ▶ Advising on control aspects of a design and ensuring that these recommendations are implemented
- ▶ Ensuring that the system meets organisational objectives
- ▶ Maintaining the quality of the delivered products and reviewing the change management process
- ▶ Assessing the effectiveness of the system
- ▶ Reviewing maintenance procedures and ensuring that adequate documentation is maintained during change implementation
- ▶ Ensuring production and source integrity



6 Specialised Systems

✂ Learning Goals ✂

- An understanding of Artificial Intelligence (AI) that includes
 - ▼ Characteristic features of AI applications
 - ▼ AI applications like expert systems, neural systems, robotics etc.
- An insight on expert systems, its components, merits and shortcomings
- An overview of data warehouse, data mining and its concept
- An understanding on Decision Support systems (DSS) that includes
 - ▼ DSS frameworks
 - ▼ Design, development and implementation issues in DSS
 - ▼ DSS trends
- Point of Sale systems
- ATMs
- EDI, E-Commerce, ERP Systems

Artificial Intelligence (AI)

Artificial Intelligence is an attempt to duplicate intelligent behaviour of the human beings in computer system on the basis of predetermined set of rules.

A few such capabilities include:

- Thinking and reasoning
- Using reason to solve problems
- Learning from experience
- Exhibiting creativity and imagination
- Handling ambiguous or incomplete information

AI applications

The applications of AI can be classified into three major categories: Cognitive Science, Robotics and Natural Languages

Cognitive Science: This is an area based on research in disciplines such as biology, neurology, psychology, mathematics and allied disciplines. It focuses on how human brain works and how humans think and learn. Applications of AI in the cognitive science are:

- **Expert Systems:** These are information systems with reasoning capability. These are discussed in detail later.

Module 4, Chapter 6

- ▶ **Learning Systems:** These are the systems that can modify their behaviour based on information they acquire as they operate. Chess playing systems is one such popular application.
- ▶ **Fuzzy logic:** These are systems that can process data that are ambiguous and incomplete. This permits them to solve unstructured problems. These systems are 'trained' to learn imprecise terminology such as those normally used by humans in their interactions. Many embedded systems such as in auto-focus cameras and energy efficient air-conditioners use fuzzy logic.
- ▶ **Neural networks:** These are computing systems modelled after the human brain. This is with reference to the mesh like network of interconnected processing elements. Though the architecture is much simpler than the human brain, it permits them to recognise patterns. Such patterns get more and more refined with data input. For example credit risk determination could be a good application for neural network systems. With data on creditworthy customers and defaulting customers, the network can generate patterns of users who are likely to be creditworthy or defaulters.
- ▶ **Genetic algorithms:** These simulate biological evolutionary processes to generate better solution to problems - particularly the kind of problems in which thousands of solutions are possible and there is a need to find a method to arrive at an optimal solution. Some of the observations such as how ants and termites collect their food have provided valuable insights.
- ▶ **Intelligent agents:** Intelligent agents are software that use built-in and learned knowledge base about a person or process to make decisions and accomplish tasks in a way that fulfils the intentions of user. Most of the modern word processing packages have a facility to observe user operations, correct his mistakes and provide useful hints depending on the context. This facility is an intelligent agent. Wizards found in MS Office are intelligent agents. Wizards are built-in capabilities that can analyse how an end user is using a software package and offer suggestions on how to complete various tasks.
- ▶ **Robotics:** This technology produces robot machines with computer intelligence and human-like physical capabilities. This area includes applications that give robots visual perception, capabilities to feel by touch, dexterity and locomotion. Robotics find expensive application in computer aided manufacturing.
- ▶ **Natural languages:** Being able to 'converse' with computers in human languages is the goal of research in this area. Interactive voice response and natural programming languages, closer to human conversation, are some of the applications. Virtual reality is another important application that can be classified under natural interfaces.
- ▶ **Virtual reality:** Virtual reality involves using multi sensory human-computer interfaces that enable humans to experience computer

simulated objects, space and activities, as they actually exist. Flight simulation for training pilots, surgery simulation for training doctors are some of the applications of virtual reality.

Auditor's Role

IS auditor needs to be concerned with the controls relevant to these systems when used as the integral part of the organizations business process or critical functions and the level of experience or intelligence used as a basis for developing the software. The errors produced by such systems would be more critical as compared to the errors produced by the traditional system.

Expert Systems

One of the most practical and widely implemented applications of artificial intelligence in business is the development of expert systems. An expert system (ES) is a knowledge based information system that uses its knowledge about a specific, complex application area to act as an expert consultant. They not only provide answers in the specific application area, but also explain their reasoning process and conclusions.

Components of expert systems

The components of expert systems are:

- ▶ **User interface:** This allows the user to interact with the system. The user presents the problem for which solutions are delivered to him. There are different ways in which a dialogue takes place between the user and the system. The most common instance is the one in which the system runs a session where a set of questions are fired to the user. The user in turn has to reply with relevant information. Here all the initiative lies with the system because it runs the whole show. The ultimate interface would be the one allowing the user to take all the initiative.
- ▶ **Interface engine:** The interface engine is that part of the program which reasons and determines the application of knowledge in the knowledge base to the facts presented in the user interface. Interface engine is the active component of an expert system and its main job is to mimic human reasoning so that the user can understand why the system has chosen a particular step. It applies two basic methodologies:
 - ▼ **Backward chaining:** The system starts with an error and then reason backwards to arrive at possible symptoms.
 - ▼ **Forward chaining:** Here the reverse action is taken. The system starts with what it has to offer and then reasons forward to determine what it can perform.

Techniques for reasoning with uncertain data input are integral to the interface engine.

Module 4, Chapter 6

- ▶ **Knowledge base:** This is the most important element of an expert system since it holds the expert problem solving knowledge. The key to the knowledge base is the way knowledge is represented. The knowledge acquired from the expert has to be represented formally. Knowledge representation deals with structuring of information and ways to manipulate it to infer additional data.

Advantages of expert systems

- ▶ The knowledge and experience of the expert is captured before he leaves the organisation
- ▶ The codified knowledge in a central repository makes it easy to share it with the less experienced in the application area
- ▶ This ensures consistent and quality decisions
- ▶ It also enhances personnel productivity

Limitations of expert systems

- ▶ Expert systems perform well in solving specific types of problems in a limited domain. When the problems involve multiple domains, expert systems become difficult to construct
- ▶ They do not have the capacity to learn and from that point of view are static in their knowledge
- ▶ Usage of specialised languages render maintenance of expert systems difficult
- ▶ Development costs of expert systems are high

Applications of expert systems

Some of the typical applications of expert systems are

- ▶ Portfolio analysis
- ▶ Insurance
- ▶ Demographic forecasts
- ▶ Help Desk operations
- ▶ Medical diagnostics
- ▶ Maintenance scheduling
- ▶ Communication network planning
- ▶ Material selection

Applications of expert systems in IS Audit

The expert systems that can be used by the auditors fall in one of the following criteria:

1. **Risk Analysis:** This expert system will evaluate materiality and various types of risks associated with the auditee.
2. **Evaluation of Internal Control:** This expert system can identify the likely exposures in the given control area.
3. **Audit Program planning:** This expert system will recommend a set of audit procedures to be conducted on the basis of auditee's characteristics and may help to evaluate the internal control system of the organization

4. Technical Advice: This expert system assists in technical advice which are encountered during audit. E.g. Confirming that the financial statements confirm the statutory regulation.

Data Warehouse

Data Warehouse is defined as a planned, integrated, managed store of relevant corporate data optimized for analysis, query and reporting purposes. The data is extracted from the operational database. A data warehouse contains historical data of a much longer period than operational database. This is the collection of enterprise data extracted from the business operations, often combined with derived or third party information. This data is stored in a separate server than the one holding the current operational database for the following reasons:

- ▶ Holding such a voluminous data of old periods will affect the online performance of the operational database.
- ▶ The purpose of data warehouse is analysis by supervisory / top management for decision making and thus may not be required by the operators during their daily regular functions and therefore the database for the historical period should not be combined with the operational database.
- ▶ The principles of Confidentiality, Integrity and Availability can be better administered if the current data is stored separately as against the historical data.
- ▶ To standardize information and its meaning
- ▶ For speedy integration of past information on the servers in the various geographical areas.
- ▶ To make available the information to the User departmental heads (owners) without framing costly and sophisticated software for extraction of the data.

The structure of the data warehouse could be:

1. Subject Oriented Data Warehouse: where the enterprise historical data related to various geographical area would be sorted and stored on the basis of a particular subject or functions viz. Data related to Sales, customer service complaints etc.
2. Integrated Data Warehouse: The total enterprise historical data is centrally stored so as to facilitate speedy access.
3. Time Variant Data Warehouse: The historical data is sorted and stored on the basis of period to have the comparison of the data for the same period amongst different locations.

The Data Warehouse is primarily composed of:

- ▶ Data sources made up of existing databases, files and external information
- ▶ Data extraction and transformation involving data cleansing and data reconstruction

Module 4, Chapter 6

- ▶ Data mart, which is a data intended for a single function or a Department on selected subjects like marketing, product etc, is created by various user departments through the process of aggregation and summarization.

In contrast to the Online Transaction Processing (OLTP) applications of operational database, the data warehouse is subject to Online Analytical Processing (OLAP). OLAP permits many operations such as

- ▶ Consolidation: Grouping and aggregation of data
- ▶ Drill-down: Ability to look into layers of details from summary, depending on the need.
- ▶ Slicing and dicing: Ability to look at the data base from different viewpoints

All these capabilities, coupled with the graphical output capability, support the top management, in their strategic decision making.

Data warehouses find application in areas such as Market analysis. The management attempts to identify patterns from the warehouse and make decisions on that basis. The process of identifying patterns in data warehouse is called data mining. When a data warehouse is not created for the entire enterprise, but only for a part of it for a specific function, it is called data mart.

Auditor's Role:

IS Auditor should keep in mind the following while conducting an audit of Data Warehouse.

1. Credibility of the source data
2. Accuracy of the source data
3. Complexity of the source data structure
4. Accuracy of extraction and transformation process
5. Access control rules
6. Network capacity for seedy access

Data Mining

Data Mining is a process of recognizing the patterns among the data in the data warehouse. IS Auditors are likely have to place more reliance on the data mining technique to assess audit risk and to collect and evaluate audit risk by

1. Detecting errors and irregularities
2. Knowledge discovery by better assessing safeguarding of assets, data integrity and effective and efficient operation of the system

Decision Support Systems (DSS)

These are information systems that provide interactive information support to managers with the use of analytical models. DSS are designed to be adhoc systems, modelled for specific decisions of individual managers.

Typical examples could be:

1. Comparative sales figures between two consecutive months for different products with the percentage variation to total sales
2. Revenue and Cost projections on the basis of certain product mix
3. Evaluation of different alternatives, leading to selection of the best one.

DSS frameworks

Frameworks are generalizations about a field that help to put many specific cases and ideas into perspective.

DSS framework will depend upon

- ▶ The extent to which the problem can be structured
- ▶ The level of management that will use the model. This corresponds to the type of decision making involved - operational, control or strategic.

Decision Support Systems

MANAGEMENT LEVEL DIMENSION	DECISION STRUCTURE DIMENSION
1) Operational Control	1) Structured
2) Management Control	2) Semi structured
3) Strategic Planning	3) Unstructured

While a structured problem is amenable to automation, a highly unstructured problem involves greater complexity in unearthing the requirements. Similarly, as the problem moves up the management decision making hierarchy, the complexity of the model increases.

Design and Development

Prototyping is the most popular approach to DSS design and development. The prototype is iteratively refined on user feedback. Therefore this can be a cost effective and speedy method.

Effectiveness of the model will depend upon

- ▶ Identification of all related factors
- ▶ The interdependencies
- ▶ The extent of their impact on the dependent variable

Implementation and use

The difficulty in implementing DSS comes out of the subjective factors that are part of the model. It is often looked upon as the product of an individual manager’s subjective views and its implementation is resisted. It is here that the change management assumes importance.

Some of the strategies recommended are:

- ▶ A phased implementation of the solution, wherever it is feasible, could be a good protection against unwillingness of users for extensive changes.

Module 4, Chapter 6

- ▶ Simpler the solution easier the implementation. While in the name of simplicity, we cannot afford to trivialise the model, unnecessary complications introduced in the solution will make its implementation difficult.
- ▶ As the design progresses, the designer should be keen on the buying-in by the users and should keep on increasing the support base for the solution. Discussing the solution with the users, as its design progresses and an explicit willingness to incorporate their valid inputs are important steps in this buy-in process.

Assessment and evaluation

The true test of a DSS lies in whether it improves the manager's decision making, which is difficult to measure in tangible terms. It has to be recognised that DSS is evolutionary in nature. DSS systems do not have a defined completion date. Hence, it would not be advisable to evaluate DSS at the end, which may not be clear. Instead, DSS should be evaluated in the incremental steps for tangible results at each step.

DSS trends

- ▶ With more sophisticated capabilities built into simple packages such as MS Excel, the use of DSS is now within the reach of medium sized organisations.
- ▶ Such easy-to-use packages have increased the availability of design talent
- ▶ The capability of PC based packages for graphical outputs have rendered the output formats user-friendlier.
- ▶ With capabilities to incorporate expert systems in DSS, the quality of the models is significantly better.

Point of Sale Systems (POS)

As the name indicates, a POS system is intended to capture data at the time and place of transaction. It is often attached to scanners to read bar codes and magnetic cards for credit card payment and electronic sales. They provide significant cost and time saving as compared to the manual methods. They also eliminate errors that are inherent in manual system. POS may involve batch processing or an online processing. These are generally observed in case of big shopping malls or the departmental shops.

In case of the batch processing, the IS auditor should evaluate the batch controls implemented by the organization and whether they are in operation, the exceptional transaction logs should also be reviewed. The internal control system should take care to ensure the accuracy and completeness of the transaction batch before subjecting the same to be updated on the corporate database. In case of online updating system, the IS auditor will have to evaluate the controls for the accuracy and the

completeness of the transactions and these controls should be more effective and exhaustive as compared to the controls in batch transfer.

Automatic Teller Machines (ATM)

An automated teller machine is a specialized form of the point of sale terminal. This is designed for unattended use by a customer of a financial institution. The ATMs generally allow cash deposits, cash withdrawals and a range of banking operations like cheque book requisition, requesting account statement etc. ATMs are generally used for use after the closing hours of the financial institution and can be located either adjacent to the location of the financial institution or may be at a distant place. The facility of ATM can be within a bank, across local banks and amongst the banks outside a region. ATMs transfer the information and money over communication lines. These systems must provide a high level of logical and physical security for both the customer and the ATM machine.

Auditor's Role

The following are the guidelines for internal controls of ATM system which auditor shall have to evaluate and report upon.

- a. Only authorized individuals have been granted access to the system.
- b. The exception reports shows all attempts to exceed the limits and these reports are reviewed by the management.
- c. The bank has ATM liability coverage for onsite and offsite machines
- d. Controls on proper storage of unused ATM cards, Controls on their issue only against valid application form from a customer, Control over custody of unissued ATM cards, Return of old/ unclaimed ATM cards, Control over activation of PINs
- e. Control on the unissued PINs, Procedure for issue of PINs, Return of PINs of returned ATM cards.
- f. Controls to ensure that PINs do not appear in printed form in association with customer account number.
- g. Access control over retrieval or display of PINs via terminals
- h. Mail cards to customers in envelopes with a return address that does not identify the Bank. Mail cards and PINs separately with a sufficiently period of time (usually three days) between mailings

EDI, E-Commerce, ERP Systems

Electronic Data Interchange (EDI Systems)

Electronic Data Interchange is the oldest form of transmitting business transactions between the business partners with dissimilar computer systems. EDI is used to transmit and exchange business documents like purchase orders, request for proposals, invoices and shipping notices in a standard machine readable format.

Module 4, Chapter 6

The advantages of EDI are:

- i) Reduction in paperwork
- ii) Improved flow of information
- iii) No necessity of reeking of data
- iv) Less errors while transmitting / exchange of information
- v) Speed in communication due to electronic transmission
- vi) Improvement in carrying out a business process.

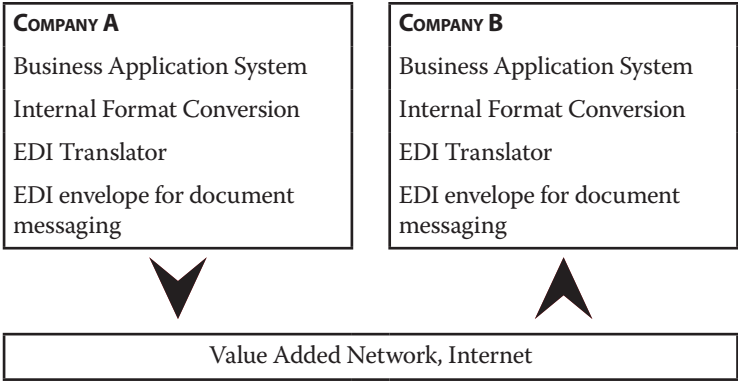
How does the EDI system function?

The EDI comprises of the following three elements:

1. **Communication Software:** moves the data from one point to another, marks the start and the end of the EDI transmission and decides how the acknowledgements are transmitted and reconciled.
2. **Translation Software:** involves conversion of data from a business application translated into a standard format, to be transmitted over the communication network, and convert this data back from the EDI format into the proprietary format of the receiver organization.
3. **EDI standard:** which specifies the standards for the transmittal of the business documents like invoices, purchase orders etc.

Traditional EDI process generally involves three functions within each trading partner's computer system.

1. **Communication handler:** Process for transmitting and receiving electronic documents between trading partners via Dial up lines, Public switched network, Multiple dedicated lines or a value added network. VAN uses computerized message switching and storage capabilities to provide electronic mail box services similar to a post office. The VAN receives all the outbound transactions from an organizations, sorts them by destination and passes them to the recipients when they log to check their mail box and receive transmissions. VAN also may perform translation and verification services.
2. **EDI Interface:** Interface function manipulates and routes the data between the application system and the communications handler. EDI interface may generate and send the functional acknowledgements, verify the identity of the partners and check the validity of the transactions by checking the transmission information against the trading partner master file. The interface consists of two components.
 - ▼ **EDI Translator** – This device translates the data between the standard format and the trading partner's proprietary format.
 - ▼ **Applications Interface** – This interface moves the electronic transactions to or from the applications systems and performs data mapping.
3. **Application System:** The programs that process the data sent to, received from, the trading partner. E.g. Purchase orders from purchasing system.



The following are the Layers for EDI transmission:

EDI LAYERS	CONSTITUENTS	
EDI Semantic Layer	Application level services	
EDI Standard Layer	EDIFACT business form standards	
	ANSI X.12 business form standards	
EDI Transport Layer	Electronic Mail	X.435 MIME
	Point to Point	FTP, TELNET
	World Wide Web	HTTP
Physical Layer	Dial Up lines, Internet	

EDI standards

There are two competing and mutually incompatible standards for EDI in existence today. They are the ANSI ASCX.12 (American National Standards Institute-Accredited Standards Committee) and UN/EDIFACT (United Nations / Electronic Data Interchange for Administration Commerce and Trade) standards.

Features of ANSI ASCX.12:

- 1. This standard was developed by ANSI, and has been adopted in the USA and some pacific Rim countries)
- 2. Standards for 250 transactions are currently available.
- 3. It is relatively rigid and inflexible when compared to EDIFACT

Features of UN/ EDIFACT:

- 1. This standard was originally developed in Europe and adopted by United Nations.
- 2. They are relatively flexible when compared to X.12
- 3. Flexibility has lead to frequent versions. Different Companies may have different versions leading to conflicts
- 4. Adopted in areas where X.12 was not adopted

Module 4, Chapter 6

- 5. Both the above standards are relatively expensive and have found the acceptance in large organizations and do not address to the needs of the small and medium size enterprises.

UN /XML

Now the effort is on to replace both X.12 and EDIFACT with XML (ex-
tensible Mark up Language). XML messages can be run on any browser
(e.g. Microsoft Internet Explorer). This in turn reduces cost of EDI and
the benefits SMEs. These initiatives go by various names like UN/XML
and ebXML (electronic business XML). The following are the features of
this emerging world standard:

- 1. Flexible, simple format
- 2. Suitable for humans and applications
- 3. Allows workflow implementation
- 4. Fusion of UN/EDIFACT and national standard (X.12)
- 5. Allows multi-lingual usage
- 6. Suitable for SMEs as well as large enterprises

Web Based EDI

Web based EDI has become popular because

- 1. Substantial reduction in the cost for small size organizations be-
cause the trade partners can use VPN on Internet as against dedi-
cated communication lines.
- 2. Its ability to attract new partners via web based sites
- 3. Improvement in the traditional EDI format
- 4. New security products are available to address issues of confidenti-
ality, integrity, authentication and non repudiation.

EDI Risks and Controls:

RISK OF EDI	EDI CONTROLS
Improper transaction authorization	Controls for inbound / outbound transactions
Integrity of EDI transactions	Encryption
Loss or duplication of EDI transac- tions	Use of sequence number for each transaction
Loss of confidentiality	Encryption
Non Repudiation	Digital signature

Auditor's Role in Auditing EDI

The IS auditor should ensure that all the controls related to the Inbound
and Outbound EDI transactions are functioning to ensure that:

- 1. Inbound EDI transactions are correctly received, translated and
passed to the correct application and is processed only once.

2. Outbound EDI transactions are authorized and are sent to the authenticated trade partners only.

To confirm the above, the auditor must ensure that:

- a. There is a control on the functional acknowledgements. Also verify that the software matches the incoming functional acknowledgements against outbound transmissions.
- b. Identify the controls for handling transaction sequencing. Ensure that a unique transaction sequence is set for each trading partner and type of transaction. Verify that there are procedures to detect out of sequence transaction conditions.
- c. Obtain a file of trading partners and verify that the software an authorization check against the trading partner master file to ensure that the trading partner number and authorized transaction types are valid.
- d. Verify that the software extracts data from the application or a flat file and reformats it in the EDI data formats in the version and release agreed upon by the Company and its trading partners. Ensure that the translator separates transactions and routes them to the appropriate application systems.
- e. Check whether the maintenance agreement for the software includes updates to new versions and releases of the X.12 standard as part of the annual maintenance and obtain a copy of the agreement.
- f. Ensure that the fields are checked for reasonableness edit checks to ensure that the data is accurate before it is routed to the appropriate application.
- g. Ensure that all inbound transactions are logged. The total of the inbound transactions received by the EDI system must be equal to the number and value of transactions forwarded and processed. Discrepancies, if any, must be accounted for and satisfactorily explained and reconciled.
- h. Ensure the continuity of message serial numbers.
- i. Review the functioning of the EDI system to ensure that functional acknowledgements are properly sent. The sender should match the functional acknowledgements with the log of the EDI messages sent.

Electronic Commerce (E Commerce):

Other than buying and selling goods on the Internet, the E Commerce involves, information sharing, payment, fulfillment and service and support.

1. Information Sharing:

The WWW provides effective medium to communicate to your customers. The organization can devise a Web Site to include the product catalogs that can be searched electronically by the prospective customers and the organization can obtain data on which products were re-

Module 4, Chapter 6

requested in searches, and how often these searches were made. A request can also be made to the visitor to the web site by asking them to provide information about themselves as they search your catalog or prepare an online order can help the web site to demographic data to product searches and information.

2. Payment:

The payment can be made through the internet by using

- a. a credit card,
- b. an electronic cheque, which has all the features of a paper check. It functions as a message to the sender's bank to transfer funds, and like a paper cheque, the message is given initially to the receiver who in turn endorses the cheque and presents it to the Bank to obtain funds.
- c. digital cash system in which the currency is nothing more than a string of digits. The bank might issue these strings of digits and debit the account with the withdrawal equal to the value of the currency (tokens) issued. The Bank validates each token with its digital stamp before transmission to the customer's account. When the customer has to spend some e-cash, he has to transmit the proper amount of tokens to the merchant who then relays them to the bank for verification and redemption. To ensure that each token is used only once, the Bank records the serial number of each token as it is spent. If the token's serial number is already recorded in the database, the Bank has detected someone trying to spend the token more than once, and would inform the merchant that it is worthless.

The small denomination digital tokens used for payment are called microcash. Microcash can be used for items such as a stock quote, a weather report, an image or even a chapter from electronic book.

3. Fulfillment:

Many companies make money by generating, transferring or analyzing the information. Documentation, program patches and upgrades are also well suited to Internet based distribution.

4. Service and Support:

Rarely does a Company's relationship with a customer end with a sale. In fact, sale may be only the beginning of the long and fruitful relationship with a customer. Not only might the customer need some sort of assistance with the product or service, but the seller may electronically obtain the feedback, suggestion and registration of the product.

The Advantages of the E Commerce are:

1. Savings in Cost
2. Saving in transaction time
3. No limitations of the geographical boundaries.

4. Larger availability of the customer base for the suppliers and larger choice to the customers
5. No restriction of timings
6. Storage or holding cost can be greatly reduced
7. Different roles for the intermediaries

The E Commerce risks are those risks connected with the transfer of any information with Internet.

RISK	CONTROL
1. Confidentiality of message	Encryption with receiver's public key
2. Identity of the sender	Encryption by sender's private key (Digital Signature)
3. Integrity of the message	Comparison of the message digest sent by the sender with the message digest converted from the received message
4. Non Acceptance of confidentiality by receiver	Encryption with receiver's public key obtained by the sender from Certifying Authority
5. Non Repudiation by sender of having sent the message	Decryption with sender's public key obtained by the receiver from Certifying Authority

Types of E Commerce Models

1. Business to Business (B to B) relationship:

B2B sites link different businesses or parts of a business. Transactions on these sites take place between industrial manufacturers, whole sellers or retailers. These transactions are of high value per customer, lesser in number, securing payment, and keeping the information private.

2. Business to consumer (B to C) relationship:

B2C sites sell products or services directly to the consumers. Transactions on these websites are in large number having small value per customer. These sites enable the customers to set prices, and business enterprises bid to offer products and services

3. Business to Employee (B to E) relationship:

Web sites developed for employees of a big enterprises gives information from the business to employees and employees feedback to business.

4. Business to Government (B to G) relationship:

This arrangement shall cover all transactions between government to business like making available certain information, circulars or forms applicable to the business and shall involve the transactions like pay-

Module 4, Chapter 6

ment of taxes by the business to the government and refund of excess taxes by the government back to the business.

5. Consumers to Consumers (C to C) relationship:

Through C2C sites, the consumer can buy and sell through each other through auctions or through other similar sites. For example vehicle of one consumer can be bought by another consumer.

6. Citizen to Government (C to G) relationship:

Citizen to Government and Government to Citizen is using the internet for accessing certain government policies, tax forms, filing Electronic information etc

7. Exchange to Exchange (X to X) relationship:

This arrangement is multiple B 2 B relationship between two merchant exchanges. For example the relationship of metal exchanges between two countries.

Enterprise Resource Planning Systems (ERP Systems)

Enterprise Resource Planning (ERP) are fully integrated corporate solutions focusing on the business applications like finance and control, production planning, sales, warehousing and logistics etc. Presently, there are many ERPs available in the market like SAP, Oracle Applications, BAAN, People Soft etc. As ERP systems are implemented by the Enterprise due to their acceptability but requires lot of changes in the present system documentation and steps, the IS auditor can evaluate the process by which the management worked out their suitability and cost benefit analysis, the change management including conversion of data from the legacy system into ERP, the training to the users on the new ERP system etc. The ERPs save lot of time by recording the business transaction only once and at the first instance only. For example, the raw materials received shall be recorded only by the Receiving Department, while the dispatches shall be recorded only by Warehouses on the basis of physical outward movement of the finished goods, the collections from the customers or debit or credit notes relating to sales shall be entered by Sales Department and the job of the accounting and finance department shall be that of reconciliation and control. The information is accessible for anybody having authorized under Access Control Rules enabling the person to know the latest position instantaneously through the networked system.

Auditor's Role

1. The IS Auditor can refer to the implementation or customization procedure to ensure that appropriate controls available in ERP are enabled while customization.

2. As the information is recorded only through the authorized persons, the responsibility for the transactions recorded and cancelled can be fixed.
3. The Auditor is required to evaluate the internal controls in the operation of the ERP as designed by the management which would be available in the respective documentation and through the interviews and observation ensure that these are actually followed at the departmental levels.

Summary

Specialised computer-based application systems or intelligent systems refer to a framework that integrates both hardware and software infrastructure in such a way that it serves as a complete solution to problems that entail human intelligence. In other words, these systems simulate the human brain in problem-solving methodologies. Continuing research and study in the field of specialised computer-based systems has resulted in evolution of Artificial Intelligence (AI), expert systems, Decision Support Systems (DSS). AI is an attempt simulate intelligent behaviour in computer system that makes a computer think, reason and make use of this reasoning in problem solving. The applications of AI can be classified into three major categories: Cognitive Science, Robotics and Natural Languages.

- A. An expert system (ES) is a knowledge based information system that uses its knowledge about a specific, complex application area to act as an expert consultant. They not only provide answers in the specific application area, but also are able to explain their reasoning process and conclusions.

Typically, an expert system comprises user interface, interface engine and a knowledge base.

Expert systems are employed in portfolio analysis, insurance, demographic forecasts, help desk operations, medical diagnostics, maintenance scheduling, communication network planning and material selection.

- B. Decision Support Systems (DSS) are information systems that provide interactive information support to managers with the use of analytical models. DSS are designed to be adhoc systems, modelled for specific decisions of individual managers. For example, a Spreadsheet package can be used for creating DSS models

Establishing and ensuring proper functioning of intelligent systems involves efficient data object management. This calls for a data management design that is capable of linking different interfaces (both software and hardware), in managing historical and statistical data. Such data management systems are referred to as data warehouses.

Module 4, Chapter 6

- C. Data warehouse is defined as a planned, integrated, managed store of relevant corporate data optimised for analysis, query and reporting purposes. The data for the data warehouse is extracted from the operational database. Data Mining is a process of recognizing the patterns among the data in the data warehouse.
- D. A Point of Sale System captures data at the time and place of transaction through scanners to read bar codes and magnetic cards for credit card payment and electronic sales. They provide significant cost and time saving as compared to the manual methods. They also eliminate errors that are inherent in manual system.
- E. Automated Teller Machines are point of sale used by a financial institution like a Bank to serve their customers for cash deposits and withdrawals. They are useful for the customers especially after business hours and at locations away from the location of the financial institution. ATM system must be provided with the highest physical and logical security.
- F. Electronic data interchange is the oldest form of transfer of information through a standard machine readable output. The EDI requires communication software, translation software and EDI standard. There are some concerns in respect of the inbound and outbound transactions. There are two competing and mutually incompatible standards for EDI in existence today. They are the ANSI ASCX.12 (American National Standards Institute-Accredited Standards Committee) and UN/EDIFACT (United Nations / Electronic Data Interchange for Administration Commerce and Trade) standards.
- G. E Commerce involve carrying out the business electronically in respect of sharing of information through B2B, B2C, B2E, B2G, C2C, X2X etc. There are concerns like confidentiality, authenticity and non repudiation, and integrity in case of E Commerce transactions. The major advantages of the E Commerce system are Saving in time, no limitation on time and geographical boundaries, avoidance of intermediaries etc.
- H. ERPs are integrated systems used by big enterprises. These give solutions to most business processes. The IS auditor must ensure that the controls available in the ERP have been enabled by the customization authority. The EPRs save lot of time by recording the business transaction only once and at the first instance only.



Questions

1. The primary function of the steering committee is:
 - A. Reviewing user requirements and ensuring that all controls are considered.
 - B. Strategic planning for computer installation.

Module 4, Questions

- C. Evaluating specific project plans for systems
 - D. Conducting a major feasibility study, when it is required.
2. In an information processing system, specific measures were introduced to improve quality. An auditor however will not be assured of the effectiveness of these measures by:
- A. A perceptible reduction in problems reported by users.
 - B. Increased satisfaction
 - C. An increase in the quality assurance budget.
 - D. A reduction in the maintenance cost of the application.
3. Which one of the following methodologies requires efficient system requirement analysis?
- A. Reverse engineering
 - B. The Delphi Design (JAD)
 - C. Joint application Design (JAD)
 - D. Traditional system development life cycle.
4. Which of the following statements is false (with regard to structured programming concepts and program modularity)?
- A. Modules should perform only one principal function.
 - B. Interaction between modules should be minimal.
 - C. Modules should have only one entry and one exit point.
 - D. Modularity means program segmentation.
5. Software quality assurance takes care of:
- A. Error prediction
 - B. Error prevention
 - C. Error detection
 - D. Error correction
6. A computerized information system frequently fails to meet the needs of users because:
- A. user needs are constantly changing.'
 - B. the growth of user requirements was inaccurately forecast.
 - C. the hardware system limits the number of concurrent users.
 - D. user participation in defining the system's requirements is inadequate.
7. Which of the following groups/ individuals assume ownership of systems development life cycle projects and the resulting system?
- A. User management
 - B. Senior management
 - C. Project Steering committee
 - D. Systems development management
8. Data flow diagrams are used by IS auditors to:
- A. Order data hierarchically
 - B. Highlight high-level data definitions

Module 4, Questions

- C. Graphically summarise data paths and storage
 - D. Portray step-by-step details of data generation
9. Which of the following would NOT normally be part of a feasibility study?
- A. Identifying the cost savings of a new system.
 - B. Defining the major requirements of the new system.
 - C. Determining the productivity gains of implementing a new system.
 - D. Estimating a pay-back schedule for cost incurred in implementing the system.
10. When auditing the requirements phase of a software, an IS auditor would:
- A. assess the adequacy of audit trails.
 - B. identify and determine the criticality of the need.
 - C. verify cost justifications and anticipated benefits.
 - D. ensure the control specifications have been defined.
11. Which phase of SDLC uses Data Flow Diagrams?
- A. Requirements
 - B. Design
 - C. Implementation
 - D. Maintenance
12. Which of the following is performed first in a system development life cycle project?
- A. Developing program flow chart
 - B. Determining system inputs and outputs
 - C. Developing design documents.
 - D. Developing conversation plans
13. In which of the following SDLC (System Development Life Cycle) phases, is the IS auditor's participation unnecessary?
- A. Feasibility study
 - B. User requirements
 - C. Programming
 - D. Manual specifications
14. In a system development project, the formal change control mechanism is begun after:
- A. Completing the system planning document
 - B. Completing the system requirement document
 - C. Completing the system design document
 - D. Completing the program coding work
15. A decision table is used in program testing to check the branching of distinct processes. It consists of:
- A. A condition stub and result

Module 4, Questions

- B. A condition stub, condition entry, action stub and action entry
 - C. An action stub and condition entry
 - D. An action stub and result
16. An IS auditor who plans on testing the connection of two or more system components that pass information from one area to another would use:
- A. Pilot testing.
 - B. Parallel testing.
 - C. Interface testing.
 - D. Regression testing.
17. A large number of system failures are occurring when corrections to previously detected faults are resubmitted for acceptance testing. This would indicate that the development team is probably not adequately performing which of the following types of testing?
- A. Unit testing
 - B. Integration testing
 - C. Design walkthroughs
 - D. Configuration management
18. An organization is developing a new business system. Which of the following will provide the MOST assurance that the system provides the required functionality?
- A. Unit testing
 - B. Regression testing
 - C. Acceptance testing
 - D. Integration testing
19. Which of the following is a primary purpose for conducting parallel testing?
- A. To determine if the system is more cost-effective.
 - B. To enable comprehensive unit and system testing.
 - C. To highlight errors in the program interfaces with files.
 - D. To ensure the new system meets all user requirements.
20. Unit testing is different from system testing because:
- A. unit testing is more comprehensive.
 - B. programmers are not involved in system testing.
 - C. system testing relates to interfaces between programs.
 - D. system testing proves user requirements are adequate.
21. Which of the following is NOT an advantage of an object-oriented approach to data management systems?
- A. A means to model complex relationships.
 - B. The ability to restrict the variety of data types.
 - C. The capacity to meet the demands of a changing environment.
 - D. The ability to access only the information that is needed.

Module 4, Questions

22. Design prototyping is more likely to be needed when:
- A. The application system to be designed is a traditional accounting system.
 - B. There is substantial uncertainty surrounding the system to be designed.
 - C. The designer believes that there is no need to develop user specification for the system to be implemented.
 - D. The SDLC approach to system development is adopted.
23. Which of the following represents a typical prototype of an interactive application?
- A. Screens and process programs
 - B. Screens, interactive edits and sample reports
 - C. Interactive edits, process programs and sample reports
 - D. Screens, interactive edits, process programs and sample reports .
24. Which of the following is a management technique that enables organizations to develop strategically important system faster while reducing development costs and maintaining quality?
- A. Function point analysis
 - B. Critical path methodology
 - C. Rapid application development
 - D. Program evaluation review technique
25. The prototyping approach does not assume the existence of:
- A. Reusable software
 - B. Formal specifications languages
 - C. Detail requirements document
 - D. Fourth-generation programming languages
26. Which of the following would be considered to be the MOST serious disadvantage of prototyping systems development?
- A. The prototyping software is expensive.
 - B. Prototyping demands excessive computer usage.
 - C. Users may perceive that the development is complete.
 - D. The users needs may not have been correctly assessed.
27. Which of the following is an advantage of prototyping?
- A. The finished system normally has strong internal controls.
 - B. Prototype systems can provide significant time and cost savings.
 - C. Change control is often less complicated with prototype systems.
 - D. It ensures that functions or extras are not added to the intended system.

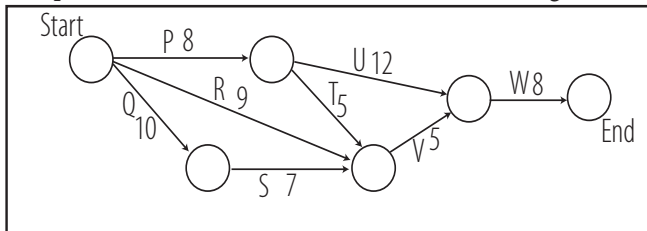
Module 4, Questions

28. Structured programming is BEST described as a technique that:
- A. provides knowledge of program functions to other programmers via peer reviews.
 - B. reduces the maintenance time of programs by the user of small-scale program modules.
 - C. makes the readable coding reflect as closely as possible the dynamic execution of the program.
 - D. controls the coding and testing of the high-level functions of the program in the development process.
29. The biggest benefit of prototyping is:
- A. Better version control
 - B. Better communication between developers and users
 - C. Increased productivity
 - D. Quicker delivery
30. Which one of the following techniques is represented by structured analysis and design?
- A. Function-oriented techniques
 - B. Data-oriented techniques
 - C. Control-oriented techniques
 - D. Information-oriented techniques
31. The critical path in a Program Evaluation Review Technique (PERT) chart is identified by:
- A. The project management team after identifying the critically of the function.
 - B. The path that has maximum slack time.
 - C. The path that has zero slack time.
 - D. Project development team after discussing with the uses.
32. Which of the following 'estimate of time' has most important relevance in PERT evaluation technique?
- A. Most likely time
 - B. Pessimistic time
 - C. Actual time
 - D. Optimistic time
33. Introduction of CASE tools in a mainframe environment provides which of the following benefit?
- A. Easy conversion of huge data
 - B. Adequate technical knowledge
 - C. Proper training personnel
 - D. Acts as supportive tools

Module 4, Questions

34. PC – based analysis and design tools are used along with mainframe computer-based tools. Identify the CASE tool that is required in this situation.
- A. Diagramming tools
 - B. Simulation tools
 - C. Export / import tools
 - D. Diagram checking tools
35. Many IT projects experience problems because the development time and / or resource requirements are underestimated. Which of the following techniques would improve the estimation of the resources required in system construction after the development of the requirements specification?
- A. PERT chart
 - B. Recalibration
 - C. Cost-benefit analysis
 - D. Function point estimation
36. Which of the following is a management technique that enables organizations to develop strategically important system faster while reducing development costs and maintaining quality?
- E. Function point analysis
 - F. Critical path methodology
 - G. Rapid application development
 - H. Program evaluation review technique
37. A significant problem in planning and controlling a software development project is determining:
- A. project slack times.
 - B. a project's critical path.
 - C. time and resource requirements for individual tasks.
 - D. precedent relationships which preclude the start of certain activities until others are complete.

Answer the questions 8 and 9 on the basis of the following PERT diagram.



38. The arrows and letters P through W in the diagram represent:
- A. events
 - B. activities
 - C. successor points

- D. predecessor points
39. Which of the following project completion paths represents the critical path?
- A. PUW
 - B. PTVW
 - C. RVW
 - D. QSVW
40. Which of the following computer aided software engineering (CASE) products is used for developing detailed designs, such as screen and report layouts?
- A. Super CASE
 - B. Upper CASE
 - C. Middle CASE
 - D. Lower CASE
41. For which of the following does the IS auditor NOT take part in the development team deliberations?
- A. Ensuring adequacy of data integrity controls.
 - B. Ensuring adequacy of data security controls.
 - C. Ensuring that there are no cost and time overruns
 - D. Ensuring that documentation is accurate life cycle project?
42. Which of the following issues requires more attention from an information Systems (IS) auditor participating in a system development life cycle project?
- A. Technical issues
 - B. Organisational issues
 - C. Behavioural issues
 - D. Contractual issues
43. After the system is developed, the auditor's objective in conducting a general review is to
- A. Determine whether a critical application system needs modification due to recent change in the status.
 - B. Conduct a test of controls to ensure that the no necessary control is omitted in the design?
 - C. Make an evaluation of the whole process to quantify the substantive test required for the specialization audit of the process.
 - D. Conduct a substantive test of the application system.
44. An auditor evaluating a software package purchase contract will NOT expect the contract to include.
- A. License cost
 - B. Maintenance cost

Module 4, Questions

- C. Operational costs
 - D. Outage costs
45. An IS auditor while conducting a post-implementation review, would look for
- A. The documentation of the test objectives
 - B. The extent of issues pointed out in the user acceptance test and the unresolved issues.
 - C. The documentation of the test results.
 - D. The log containing the problems reported by the users.
46. The use of coding standards is encouraged by IS auditors because they:
- A. define access control tables.
 - B. detail program documentation.
 - C. standardize dataflow diagram methodology.
 - D. ensure compliance with field naming conventions.
47. An IS auditor involved as a team member in the detailed system design phase of a system under development would be MOST concerned with:
- A. internal control procedures.
 - B. user acceptance test schedules.
 - C. adequacy of the user training program.
 - D. clerical progress for resubmission of rejected items.
48. An IS auditor who has participated in the development of an application system might have their independence impaired if they:
- A. perform an application development review.
 - B. recommend control and other system enhancements.
 - C. perform an independent evaluation of the application after its implementation.
 - D. are actively involved in the design and implementation of the application system.
49. The primary role of an IS auditor in the system design phase of an application development project is to:
- A. advise on specific and detailed control procedures.
 - B. ensure the design accurately reflects the requirement.
 - C. ensure all necessary controls are included in the initial design.
 - D. advise the development manager on adherence to the schedule.
50. Which of the following tasks would NOT be performed by IS auditor when reviewing systems development controls in a specific applications?
- A. Attend project progress meetings.

Module 4, Questions

- B. Review milestone documents for appropriate sign-off.
 - C. Compare development budgets with actual time and amount spent.
 - D. Design and execute testing procedures for use during acceptance testing.
51. E-cash is a form of electronic money that:
- A. can be used over any computer network.
 - B. utilizes reusable e-cash coins to make payments.
 - C. does not require the use of an Internet digital bank.
 - D. contains unique serial numbering to track the identity of the buyer.
52. Which of the following statements is incorrect?
- A. Expert systems are aimed at solving problems using an algorithmic approach
 - B. Expert systems are aimed at solving problems that have irregular structure
 - C. Expert systems are aimed at solving problems which have incomplete information
 - E. Expert systems are aimed at solving problems of considerable complexity
53. Which of the following is a characteristic of a decision support system (DSS)?
- A. DSS is aimed at solving highly structured problems.
 - B. DSS combines the use of models with non-traditional data access and retrieval functions.
 - C. DSS emphasizes flexibility in the decision making approach of users.
 - D. DSS supports only structured decision-making tasks.
54. Which of the following is false with regard to expert systems?
- A. Expert system knowledge is represented declaratively
 - B. Expert system computations are performed through symbolic reasoning
 - C. Expert systems knowledge is incorporated in the program control
 - D. Expert systems control their own actions
55. Which of the following statements pertaining to data warehouses is FALSE?
- A. A data warehouse is designed specifically for decision support.
 - B. The quality of the data in a data warehouse must be very high.
 - C. Data warehouses are made up of existing database, files and external information.
 - D. A data warehouse is used by senior management only because of the sensitivity of the data.

Module 4, Questions

56. Use of asymmetric encryption over an Internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:
- A. Customer over the authenticity of the hosting organization.
 - B. Hosting organization over the authenticity of the customer.
 - C. Customer over the confidentiality of messages from the hosting organization.
 - D. Hosting organization over the confidentiality of message passed to the customer.
57. Which of the following concerns about the security of an electronic message would be addressed by Digital Signatures?
- A. Unauthorised reading
 - B. Theft
 - C. Unauthorised copying
 - D. Alteration
58. A (B 2 C) E commerce web site as part of its information security program, wants to monitor, detect and prevent hacking activities and alert the system administrator when suspicious activities occur. Which of the following infrastructure components could be used for this purpose?
- A. Intrusion detection systems
 - B. Firewalls
 - C. Routers
 - D. Asymmetric encryption
59. Fuzzy Logic is most effective when:
- A. Used to develop decision support system
 - B. Combined with neural network technologies
 - C. Used to build hard disc controllers
 - D. Used to design memory caches
60. Which of the following is not a subsystem of the decision support system?
- A. Language system
 - B. Knowledge system
 - C. Transaction processing system
 - D. Problem processing system

Answers

QUESTION No	1	2	3	4	5	6	7	8	9	10
ANSWERS	B	C	D	D	C	D	A	C	B	D

Module 4, Questions

QUESTION No	11	12	13	14	15	16	17	18	19	20
ANSWERS	B	B	C	B	B	C	B	C	D	C

QUESTION No	21	22	23	24	25	26	27	28	29	30
ANSWERS	B	B	D	C	C	C	B	B	B	A

QUESTION No	31	32	33	34	35	36	37	38	39	40
ANSWERS	C	A	A	C	D	C	C	B	D	C

QUESTION No	41	42	43	44	45	46	47	48	49	50
ANSWERS	C	C	C	D	B	D	A	D	C	C

QUESTION No	51	52	53	54	55	56	57	58	59	60
ANSWERS	D	A	C	C	C	A	D	A	C	C

Reference Material

- ▶ “Component – Based Development: Approaching the Promised Land of Component Reuse” Martin L. Griss, Ivar Jacobson, ADTmag.com, June 2001
- ▶ A Guide to the Project Management Body of Knowledge, The Project Management Institute, USA 2000
- ▶ Information Systems Control and Audit, Ron Weber, Prentice Hall, USA, 1999, chapter 4.
- ▶ Information Technology Control and Audit, Frederick Gallegos, Daniel P Manson and Sandra Allen-Senft, Auerbach USA, 1999
- ▶ Object – oriented Software Measures, Clark Archer, Michael Stinson, Software Engineering Institute, CMU/SEI – 95 – TR - 002, USA, April 1995
- ▶ Requirements Engineering and Management, Jim Highsmith, Nancy R. Mead, Daniel J. Mosley, Balasubramaniam Ramesh, Lou Russell and Karl E. Wieggers, Cutter Information Corp; USA, July 2000
- ▶ Software Architecture Documentation In Practice: Documenting Architectural Layers, Felix Bachmann, Len Bass, Jeromy Carriere, Paul Clements, David Garlan, James Ivers, Robert Nord, Reed Little Software Engineering Institute, CMU /SEI – 2000 – SR – 004, USA March 2000
- ▶ Software Project Survival Guide, Steve McConnell, Microsoft Press, USA, 1998.

Module 4, Questions

- ▶ Software Testing and Software Development Lifecycles, IPL Information Processing Limited 1996
- ▶ Spiral Development: Experiences, Principles and Refinements, Spiral Development Workshop, 9 February .2000, Software Engineering Institute Special Report CMU/SEI –2000-SR – 008, 2000
- ▶ A Standard for Auditing Computer Applications, Martin A Krist, Auerbach Publishers, Massachusetts, USA 1999
- ▶ Taking Stock of Component Teahnology, David Chappell, Chappell & Associates USA, June 1999.



Module 5: Business Continuity Planning

1 Introduction to BCP

✂ Learning Goals ✂

To understand:

- ▶ The need for BCP.
- ▶ The various types of disasters and their impact.
- ▶ The various emerging laws, regulations and standards relating to BCP.

Need for BCP/DRP

“I am sorry, but the system is down.”

How often does one hear these words while requesting a service? This phrase reflects the failure of a system on which a business and its customers have become dependant. Information and telecommunications systems have come to play a central role in the conduct of a modern business. They connect the business with other businesses and more importantly with their customers. For example, the railway reservation system would collapse without a functioning information and telecommunications system. The stock market is virtually paperless. Banks and credit card companies have moved to an era where the customer rarely needs to set foot in the branch premises. Manufacturing industries too are now interconnected as never before. Order entry, engineering, design, purchasing and inventory management, to name just a few, are now closely coupled with the factory shop floor.

This dependence on systems means that all enterprises should have contingency plans for resuming operations for those situations where operations have been disrupted for any reason, including when an unforeseen man-made or natural disaster occurs.

Many businesses processes support critical areas such as health, safety and even lives on occasion. Organizations that run such processes have an ethical duty, often reinforced by law, to ensure that steps are taken to ensure the continuity of operations in the event of disruptions.

An enterprise may choose to assess, plan and maintain its own contingency and recovery or continuity plan solutions. However, the trend in recent years has been to outsource contingency and business continuity plan solutions.

Module 5, Chapter 1

A distinction may be drawn between business continuity planning and disaster recovery planning. A business continuity plan (BCP) aims to sustain mission critical business processes during an unplanned interruption event. A disaster recovery plan (DRP) is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss. A DRP is usually focussed on an IT or other operational facility. The key difference between the two plans lies in their scope. BCP includes DRP, more commonly, a BCP includes several DRPs.

It should be noted that, the objective of BCP is not just to develop a plan but to acquire a permanent, ongoing capability. Ron Weber calls disaster recovery plan and insurance as controls of last resort.

Types of Disasters

Disaster Events

A disaster can be defined an unplanned interruption of normal business process. More comprehensively a disaster can be defined as a disruption of business operations that stops an organization from providing its critical services caused by the absence of critical resources.

The critical resources could be:

- ▶ People and skill sets
- ▶ Facilities
- ▶ Communications
- ▶ Power (Nearly one-third of all disruptions are caused by loss of power.)
- ▶ Data/Information
- ▶ Information Systems

A BCP is designed to counter various kinds of threats. A “threat” is the potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. A threat-source is any force or phenomenon that could degrade the availability, integrity or confidentiality of an Information Systems resource, system or network. For example, a hacker is a threat source, an unauthorised system access is a threat. Given below is an illustrative list of threats and threat-sources that a BCP can guard against:

- ▶ **Power failure:** The loss of the electrical power supply to the information systems.
- ▶ **Communication failure:** The inability to transfer information to and from the organization through the defined system parameter.
- ▶ **Loss of Data Integrity:** A realized, or perceived possible, alteration of the data and/or information maintained by or consisting of the specified asset.

- ▶ **Accidental Errors:** Improper use of information technology not due to malicious intent but because of incorrect use.
- ▶ **Computer Virus:** A program, or part of a program, which spreads by attaching itself to “healthy” programs. After infection, the program may perform a variety of undesirable functions.
- ▶ **Abuse of Access Privileges by Employees:** Employees are authorized by the security policy of the organization and further restricted by their job responsibilities to perform a small selection of functions with the information system. This category covers those acts which may be performed but which are not authorized.
- ▶ **Abuse of Access Privileges by Other Authorized User:** Apart from employees, there may be other external users such as contract staff and customers, who may have authorizations to perform selected operations, restricted by their roles. There is a possibility that they may exceed these restrictions and perform operations they are not authorized.
- ▶ **Successful Unauthorized System Access by Outsider:** This refers to outsiders, who do not have any authorization to access the system. There is a possibility of their using, and possibly destroying, information system resources. “Hackers” fit within this threat description.
- ▶ **Natural Disasters:** Those occurrences, other than fire and which are not man-made, which degrade some aspect of the information system. Examples: flooding, cyclones, etc.
- ▶ **Theft or Destruction of Computing Resource:** A primary resource of the organization is the computing capability of its information systems. This threat addresses the unauthorized use of this resource and the destruction of this resource - through physical or other means.
- ▶ **Destruction of Data:** Data here is not confined to that used or generated by business applications. Apart from this crucial information, an organization possesses several other information such as manuals and knowledge repositories. A threat may destroy any of these such information, or simply prevent the organization from using it.
- ▶ **Non-disaster downtime:** This covers those times when the information system is unavailable for use not caused by disaster. Example of this would be preventive maintenance, downtime caused by system upgradation, etc.

Classification of Disasters

The disasters are usually classified as Natural or Technological (man-made).

- ▶ **NATURAL DISASTERS** are those caused by natural events, often related to weather, that pose threats to lives and property. Natural disasters include earthquakes, floods, wildfires, landslides, high winds, tornados, and cyclones.

Module 5, Chapter 1

- ▶ **TECHNOLOGICAL DISASTERS** or man-made emergencies are those caused by tools, machines and substances that are used by man. These may due to human error— intentional or accidental. Power failures, explosions, airplane crashes, electrical fires, chemical spills, bomb and terrorist attacks, structural failures, and nuclear emergencies are some examples of man-made disasters.

Impact of Disasters

The impact of a disaster may be one or more of the following:

- ▶ **Loss of human Life:** The extent of loss depends on type and severity of the disaster. Protection of human life is, the overriding principle behind most continuity plans.
- ▶ **Loss of Productivity:** When a system failure occurs, employees may be handicapped in performing their functions. This could result in productivity loss for the organization.
- ▶ **Loss of Revenue:** For many organisations like railways, airlines, banks, stock brokers and call centres, the effect of even a relatively short breakdown, cause huge revenue losses.
- ▶ **Loss of Market Share:** Given the competitive environment that prevails in many a industry, the inability to service customers could result in loss of marker share. For example, consider a prolonged failure of the services of a cellular phone company; this may result in many customers changing over to a different provider.
- ▶ **Loss of Goodwill and Customer Confidence:** If the disruption to a company is long enough or if a systems failure occurs often, the customers lose faith in the company. By not preparing for contingencies the company proves to be unreliable and loses customer's trust. Frequent loss of operational capability can severely damage the company's image as a reliable service provider and partner.
- ▶ **Litigation:** Laws, regulations, and contractual obligations govern the conduct of a business. Failure to provide safeguards that ensure the continuity of operations may bring penal action by regulatory bodies or lawsuits from trade partners who are adversely affected.

Steps in Developing a Business Continuity Plan

The process of framing a BCP is outlined below. The first step is initiation, followed by a risk assessment, choosing a recovery strategy, development and implementation, and lastly testing and validation.

- ▶ **Initiate:** This step commits management, sets expectations and establishes the basis for a successful BCP. Activities include establishment of a high-level BCP strategy, setting plan expectations, obtaining appropriate commitments, selecting the appropriate participants and establishing an efficient work plan.

- ▶ **Perform Risk Assessment:** A risk assessment is carried out to determine the extent of the potential threat and the risk associated with system. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process, and in finalizing the recovery strategy. This process documents each business unit's critical processes and components and identifies existing and potential disaster-mitigating systems/procedures, both internal and external. This includes understanding the process flow of each business unit, determining the critical recovery time period, defining the critical resources of each business unit and identifying exposures and existing containment measures. The information found in this phase will be the basis for the construction of strategies and the BCP.
- ▶ **Choose Recovery Strategy:** This step includes the following activities:
 - ▼ Identification of a recovery strategy.
 - ▼ Definition of notification procedures.
 - ▼ Definition of procedures for activating contingency plans.
 - ▼ Identification of recovery teams for each core business process.
 - ▼ Identification of appropriate course of action for the survival of the critical components of the business. These include strategies to protect computer systems, communications, staff, facilities, equipment, office supplies, market share, and continuity of suppliers.
- ▶ **Develop and Implement Plan:** Based on the recovery strategy selected, a detailed business continuity plan is developed, addressing all issues involved in recovering from a disaster. The BCP puts together a sequence of actions that counteract or mitigate the effects of the threats or risks identified in the Risk Assessment phase. It creates procedures that will re-establish the critical components of the business in the least possible time, and at the lowest cost to the business. The plan must be developed by the user using familiar terms and with references to sources of resource repair or replacement services. The plan should be easy to navigate and be understood by all participants of the recovery process.
- ▶ **Test, Validate and Maintain:** This step focuses on developing plans to test and validate the company's business continuity plan. This phase evaluates the effectiveness of procedures and access to resources through simulation of disaster. Each procedure and resource must be evaluated to determine if it will be effective during a real disaster situation. The results of the evaluation will be used to update the BCP. Periodically, the plan will need to be reviewed and amended to reflect changes in priorities, staff, equipment, and procedures.

Law and Standards

The legal framework for BCP is still evolving. Currently, BCP mandates have emanated from independent regulatory bodies and their jurisdiction is confined to specific industries. A comprehensive legislation encompassing all business segments is yet to emerge. For example, banks and financial institutions must comply with the dictates of the Reserve Bank of India which currently provide broad guidelines that require them to develop means to reduce the impact of system downtime. Currently, these guidelines are recommendatory and not mandatory. The bank management is directly responsible for determining critical functions at the bank, assessing the risk and potential impact of a loss of IT support for those functions, and developing plans to reduce the risk and/or impact of such a loss.

Foreign Legislation

While Indian organisations are not directly covered by foreign (specifically American) legislation, it is worthwhile to consider them briefly for two reasons. Firstly, many American companies outsource certain operations to Indian companies, which means that these companies are required to meet certain obligations that arise from these laws. Secondly, it is likely that sooner or later, the Indian Government may enact legislation that is analogous to US (United States) legislation.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) of USA. HIPAA aims to make the health care industry more efficient through the increased use of standard electronic transactions (such as claims and insurance eligibility requests) for health care administration. Along with the regulations for the standardization of the transactions, there are regulations to protect the privacy and security of health care information. HIPAA requires safeguards for the protection of “electronic personal health information” (ePHI) in three general areas, Administrative, Physical, and Technical, with specific implementation requirements in each area.

HIPAA also requires that the health care service provider obtain assurances that ePHI entrusted to a third party is protected. It does not create an obligation on the covered entity to proactively audit the third party for compliance with the assurances.

GBL and The Expedited Funds Availability Act

Another American law, the Gramm-Leach-Bliley (GBL) Act of 1999, requires regulatory agencies establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards for the security and confidentiality of customer records and information.

The Expedited Funds Availability Act, enacted by the U.S. Controller of Currency, requires certain financial institutions to have a demonstrable business continuity plan to ensure prompt availability of funds.

Sarbanes-Oxley Act

Sarbanes-Oxley Act of 2002 (“SOX”), was enacted in the wake of Enron and other debacles to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. Section 302 of the Act requires the chief executive and chief financial officer to sign off, on a quarterly basis, on the effectiveness of their company’s disclosure controls and procedures. If their evaluation identifies any material deficiencies, significant internal control changes or fraud involving management, they must disclose that information to the auditor and audit committee.

Section 404, requiring the Securities and Exchange Commission (“SEC”, the American stock exchange regulator) to adopt rules requiring the management of a company to present an internal control report in the annual report containing: (1) a statement of the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) an assessment, as of the end of the company’s most recent fiscal year, of the effectiveness of the company’s internal control structure and procedures for financial reporting. Section 404 also requires the company’s auditor to attest to, and report on, management’s assessment.

The law therefore requires that a company’s processes, systems, and controls must make available all material information needed for fair presentation and disclosure in its reports to regulatory bodies, including the update of accounting estimates with current and reliable information. On a more strategic scale, business continuity methodology and approach of an organization must be agreed to by management as the foundation for mitigating financial and reputation risk posed by business interruption.

Standards

GASSP

The Generally Accepted System Security Principles (GASSP) were assembled to meet US Government needs and was sponsored by The International Information Security Foundation (I2SF). GASSP is intended to provide authoritative point of reference and legal reference for information security principles, practices, and opinions. These principles were modelled after those that support and sustain the Generally Accepted Accounting Principles (GAAP) and similar models of the accounting profession. GASSP relates to physical, technical and administrative information security and encompasses “Pervasive”, “Broad

Module 5, Chapter 1

Functional”, and “Detailed Security Principles”. The Pervasive Principles provide general guidance to establish and maintain the security of information. These principles form the basis of Broad Functional Principles and Detailed Principles. One such Broad Functional Principles relates to “Operational Continuity and Contingency Planning” which states that “Management shall plan for and operate Information Technology in such a way as to preserve the continuity of organizational operations”. GASSP is aimed at general management as well as information security specialists, and are freely downloadable from the Internet.

ITIL

Information Technology Infrastructure Library (ITIL), a UK body, is a collection of best practices in IT service management, consisting of a series of books giving guidance on the provision of quality IT services. ITIL is drawn from the public and private sectors internationally, supported by a comprehensive qualification scheme and accredited training organisations. It includes descriptions of best practice in information security management as well as other related disciplines.

Basel Committee on e-Banking

The Basel Committee of Bank of International Settlements (BIS), established by the central-bank Governors of the Group of Ten (advanced) countries at the end of 1974, formulates broad supervisory standards and guidelines and recommends statements of best practice for financial institutions.

In July 2003 the Basel Committee published its principles for electronic banking; principle number 13 declares “Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services”. The Committee underlines that banks should also ensure that periodic independent internal and/or external audits are conducted about business continuity and contingency planning. The requirements are spelt out in Appendix VI relating to “Sound Capacity, Business Continuity and Contingency Planning Practices for E-Banking”:

- ▶ All e-banking services and applications, including those provided by third-party service providers, should be identified and assessed for criticality.
- ▶ A risk assessment for each critical e-banking service and application, including the potential implications of any business disruption on the bank's credit, market, liquidity, legal, operational and reputation risk should be conducted.
- ▶ Performance criteria for each critical e-banking service and application should be established, and service levels should be monitored against such criteria. Appropriate measures should be taken to ensure that e-banking systems can handle high and low transaction

volume and that systems performance and capacity is consistent with the bank's expectations for future growth in e-banking.

- ▶ Consideration should be given to developing processing alternatives for managing demand when e-banking systems appear to be reaching defined capacity checkpoints.
- ▶ E-banking business continuity plans should be formulated to address any reliance on third-party service providers and any other external dependencies required achieving recovery.
- ▶ E-banking contingency plans should set out a process for restoring or replacing e-banking processing capabilities, reconstructing supporting transaction information, and include measures to be taken to resume availability of critical e-banking systems and applications in the event of a business disruption.

Basel II Capital Accord

In June 2004, Basel Committee issued the International Convergence of Capital Measurement and Capital Standards: A Revised Framework (better known as “Basel II Capital Accord”). The objective of the new Accord is to encourage financial firms to be more proactive and forward looking in their financial activities. Basel II will enhance risk awareness and put more emphasis on the importance of good risk measurement and management and properly ensure appropriate capital reserve requirements. To meet the requirements of the Accord, banks must demonstrate that they have an overall data architecture that integrates the various business functions from risk management to finance to operations.

A focus of the Accord is on operational risk and more accurate measurement of credit risk exposure. Banks are encouraged to protect themselves adequately against potential losses. The scale and complexity of data requirements for ongoing compliance with the more advanced approaches is considerable. And even though the Accord implementation date is December 31, 2006, banks must start capturing and storing historic data immediately in order to comply with the Accord's requirements. Adopting the more advanced approaches of Basel II involves putting in place an operational and credit risk management framework with the skills, processes, and systems to store, analyse, and interpret vast amounts of data in real time. The banks will be required to address operational risk through a solid information infrastructure and business-continuity functions and address the credit risk by enabling business functions to use the same underlying data for different business processes.

SAS 70

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an auditing standard developed by the American Institute of Certified

Module 5, Chapter 1

Public Accountants (AICPA). A SAS 70 audit or service auditor's examination puts a service organization through an in-depth audit of their control activities, which generally include controls over information technology and related processes. In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 (USA) make SAS 70 audit reports even more important to the process of reporting on effective internal controls at service organizations.

SAS No. 70 is generally applicable when an auditor (called the "user auditor") is auditing the financial statements of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres, or other data processing service bureaus.

However, SAS 70 is not a pre-determined set of control objectives or control activities or standards that service organizations must achieve. This is main criticism against SAS 70. In a SAS 70 audit, the service organization is responsible for describing its control objectives and control activities that might be of interest to auditors in user organizations. If an organization does not have a security policy covering a particular area, or has one that allows ineffective security, the SAS 70 audit report would contain a favorable opinion because the control activities (none) matched the stated control objectives (none).

COBIT

COBIT (Control for Objectives Information and related Technology) is a reference framework used as a basis for establishing a method of internal control over matters of a company's information technology and information systems. COBIT is also being adopted as a IT governance framework by many organisations. COBIT is based on the control objectives set out by the Information Audit Systems and Control Foundation (ISACF) and has been drawn up and developed using international technical, professional, regulatory and industry specific standards as a basis. As in the case of the ISO standard, the resulting control objectives are considered to be "good or best practices", i.e. they are agreed on by experts, applicable and generally accepted for the information systems of any company.

The COBIT structure is based on the premise that, in order to provide the information necessary for an organization to achieve its business objectives, its IT resources must be managed by means of a set of naturally grouped processes. COBIT is a three level hierarchy (domains, processes and activities or tasks), with 4 domains in the uppermost level, Planning

and Organization (PO), Acquisition and Implementation (AI), Delivery and Support (DS), and Monitoring (M). There are 34 control objectives in the middle (processes) level, and 318 detailed control objectives in the lowest (task) level. “Control objective” is defined as “A statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.” COBIT also provides an Audit Guideline for each of these 34 high-level control objectives to match the review of the organisation’s existing IT processes against the recommended detailed control objectives to provide management assurance and/or advice for improvement.

One of the high-level control objectives is focused on BCP: “DS4: Ensure Continuous Service.” DS4’s objective is the control over the IT process ensuring continuous service to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption. DS4 is enabled by having an operational and tested IT continuity plan which is in line with the overall business continuity plan and its related business requirements. The continuity plan should take into consideration:

- ▶ Criticality classification
- ▶ Alternative procedures
- ▶ Back-up and recovery
- ▶ Systematic and regular testing and training
- ▶ Monitoring and escalation processes
- ▶ Internal and external organisational responsibilities
- ▶ Business continuity activation, fallback and resumption plans
- ▶ Risk management activities
- ▶ Assessment of single points of failure
- ▶ Problem management

Control objective DS4 is translated into 13 specific controls for the BCP. The control objectives are available in open standard format, and can be downloaded from the ISACA website (<http://www.isaca.org>).

ISO/IEC Technical Report (TR) 13335

ISO/IEC (International Electrotechnical Commission) Technical Report (TR) 13335, Guidelines for the Management of IT Security (GMITS), 13335-2: Managing and Planning IT Security, contains requirements for procedural security, including business continuity.

ISO 9002

This quality assurance model applies to organizations that produce, install, and service products. It implies industry standards for IT Security and the broader subject of general product security, including continuity planning for IT systems – both as products themselves and as environmental support – and all other aspects of business operations (physi-

Module 5, Chapter 1

cal, environmental, personnel) whose disruption would affect product security.

ISO/IEC 17799:2000

ISO/IEC (International Electrotechnical Commission) 17799:2000, 2000 Information Technology – Code of practice for information security management, an international version of British Standard 7799-1:1999, was published in December 2000. It contains 10 major sections, one of which is business continuity management (Section 11). However, parts of Physical and Environmental Security (7), Asset Classification and Control (5), and Security Policy (3) would also apply.

The Indian National Certification standard equivalent to ISO/IEC 7799 is called the IS 15150.

Summary

For many organisation the value of “information” exceeds the value of “fixed assets” that are traditionally reported in the annul reports. Continued access to the information asset is therefore a pre-condition for the well being and survival of the organisation. As a corollary, inability to access the information asset constitutes a disaster.

Legislative bodies and international standards setting bodies are now setting compliance requirements and standards for protecting this information asset. As a consequence of globalisation, legislative requirements in advanced countries often tend to have repercussions in India.

Most of the standards and compliance requirements that are now emerging are focussed on specific industries like financial institutions and healthcare. However the scope of some of the recently formulated standards like ISO/IEC 17799 are very broad and encompass all types of organizations.



2 Risk Assessment

✂ Learning Goals ✂

To understand:

- ▶ The objectives of risk assessment.
- ▶ The process of risk assessment.

Introduction

Risk assessment seeks to identify which business processes and related resources are critical to the business, what threats or exposures exist to cause an unplanned interruption of business processes, and what costs accrue due to an interruption.

There are various analytical procedures that are used to determine the various risks, threats, and exposures faced by an organization. These are known by various names, such as Business Impact Analysis (BIA), Application Impact Analysis, Threat and Exposure Analysis, Risk Impact Analysis and so on. While many authors and practitioners maintain subtle differences between these terms, this discussion subsumes all these activities under Risk Assessment.

Risk assessment consists of two basic operations: data collection and data analysis. The data collected in risk assessment should include a comprehensive list of business processes and their resource dependencies. With this data collected and analyzed, risk assessment can commence. The basic process of risk assessment, for the purpose of BCP, involves asset identification and prioritization, threat identification and exposure assessment and the formulation of the objectives of the BCP. A team of experts representing managerial, technical and legal experts are constituted for the purpose of Risk Assessment.

Objectives of Risk Assessment

The objectives of risk assessment include:

- ▶ **CRITICALITY PRIORITIZATION.** Identifying business functions or processes and their associated resource requirements. Prioritizing business processes according to their time-sensitivity and criticality.
- ▶ Estimating the **CRITICAL RECOVERY TIME PERIOD** (also called “Recovery Time Objectives” or “Maximum Tolerable Downtime”) of the business process. The critical recovery time period is the maximum amount of time allowed for the recovery of the of the business function. This is the amount of downtime of the business process

that the business can tolerate and still remain viable. If this time is exceeded, then severe damage to the organization will result.

Asset Identification and Prioritization

Individuals, primarily from the business unit, are the main source of data on all aspects of business operations and assets. For this reason, identifying knowledgeable individuals to be interviewed and developing interview questions are critical parts of the planning process that require careful attention and close coordination between the business unit manager and the senior management. A wide array of individuals ranging from senior managers to security specialists and contractors are interviewed. Midlevel managers from key business units are also interviewed, including individuals with knowledge of legal, safety, personnel, and operations matters, as well as related processes. The business managers are asked to usually asked too identify, based on their knowledge of the business unit's operations, the most important systems for their business units.

Risk Ranking

The ability of a company to cope with interruption of a business process determines the **TOLERANCE** of the business process. This tolerance depends on the length of the disruption and may also be linked to the time of the day or month an interruption occurs. Risk Assessment, generally, assumes that a disruption will occur at the worst possible time. In practice, tolerance is usually expressed as a monetary amount – the cost to the company if the business process is interrupted for a given unit of time. This cost of interruption is inversely related to the tolerance. The various business processes may be classified on the following spectrum of tolerance based on their critical recovery time period.

- ▶ **Critical.** These are functions that cannot be done manually under any circumstances. Unless a company locates identical capabilities to replace the damaged capabilities, these functions cannot be performed. These functions have zero or very low tolerance to interruption and consequently, the cost of interruption is very high. Thus, for critical functions, the company would need to arrange to have access to hardware comparable to its own, and in the event of an emergency, plan to transfer the function to the backup hardware to resume processing.
- ▶ **Vital.** These functions can be performed manually but only for a brief period of time. There is relatively higher tolerance to interruption as compared to critical functions and consequently somewhat lower costs of interruption. The functions classified as vital can withstand a brief suspension of operations but cannot withstand an extended period of downtime.

- ▶ **Sensitive.** These processes can be carried out by manual means for an extended period, though with some difficulty. They may require additional staff to perform and when restored, may require considerable amount of time to restore the data to a current or usable form.
- ▶ **Non-Critical.** These processes have a high tolerance to interruption and can be interrupted for an extended period of time with little or no adverse consequences. Very little time is required to restore the data to a current or usable form.

The criticality of a business process extends to resources that support the process. In most cases, it is safe to categorize certain infrastructure components, including electrical power systems, communications networks, and other fundamental resources required by all business processes, as critical. Without backups or manual means of control, a loss of any of these systems at any time may represent a total cessation of normal business operations. Engineers call these resources “single points of failure”. Within any complex system, there are usually components or processes that, if not replicated or otherwise backed up by redundant capabilities, represent points of failure for the entire system. A large part of disaster avoidance planning comes down to identifying single points of failure wherever they exist and eliminating them.

Threat Identification

Once the criticality of the various business processes has been assessed, the next step is the identification and classification of threats and threat sources. A threat is the potential for a particular threat-source to successfully exploit, accidentally or intentionally, a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source is defined as any circumstance or event with the potential to cause harm to an IT system. The threat-sources are natural or human. A threat-source does not present a risk when there is no vulnerability that can be exploited.

In determining the likelihood of a threat, one must consider threat-sources, existing and potential vulnerabilities and existing controls. To help ensure that all possible threats are considered, some organisations have established a separate corporate group that develops and maintains threat data for use by the entire organisation, including risk assessment teams. This group collects threat data from internal and external sources, including government agencies. Based on this information, the group develops a “baseline threat statement” that identifies the possible threats from outsiders, insiders (employees and support personnel), and system-induced events (faulty processes).

In developing scenarios, risk assessment teams consider how current organizational procedures or technical applications may compromise the

organization's information resources and ultimately damage the company. Considerations include disclosure of information to unauthorized individuals and organizations, loss of information, and inability to access company information due to computer malfunction or loss of communications. As part of this, the team considers the baseline threat statement, to which specific local threat data have been added.

Exposure (Vulnerability) Assessment

The organization should analyse the critical resources, assets and threats identified in the previous steps and determine the disruption or impact on a given asset or resource, if the resource were impacted by any of the threats identified. The analysis should evaluate the impact of the outage in two ways.

The effects of the disruption may be tracked over time. This will enable the organization to identify the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.

The effects of the disruption may be tracked across related resources and dependent systems, identifying any cascading effect that may occur as a disrupted system affects other processes that rely on it. The organization should determine the optimum point to recover the IT system by balancing the cost of the inoperable system against the cost of resources required for restoring the system.

The cost and time of disruption and acceptable disruption time enable the organization to develop and prioritize recovery strategies that will be implemented during contingency plan activation. For example, if it is determined that a system must be recovered within four hours, the organization would need to adopt measures to meet that requirement. Similarly, if most system components could tolerate a 24-hour disruption but a critical component could be unavailable for only eight hours, the organization would prioritize the necessary resources for the critical component. By prioritizing these recovery strategies, the organization can make more informed, specific decisions regarding contingency resource allocations and expenditures, saving time, effort, and costs.

This step can provide the organization with vital information regarding system availability and recovery requirements. In some cases, the disruption impacts identified in this step can be minimised through preventive measures that detect and/or reduce impacts to the system. Where feasible and cost-effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption.

Specification of Objectives

In this step, a set of objectives to guide the development of BCP are formulated. The goal is to eliminate exposures, if possible and to minimize the effects of those that cannot be eliminated. Risk mitigation, involves prioritizing, evaluating, and implementing the appropriate controls as recommended by the risk assessment process. Because the elimination of all risks is usually impractical or impossible, it is the responsibility of senior management and functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease risk to an acceptable level, with minimal adverse impact on the resources and mission of the organisation.

Controls that could mitigate or eliminate the identified risks, as appropriate to the operations of the organization are recommended. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- ▶ Effectiveness of recommended options (e.g., system compatibility)
- ▶ Legislation and regulation
- ▶ Organizational policy
- ▶ Operational impact
- ▶ Safety and reliability.

These recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all possible recommended controls can be implemented. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, or some other justification, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

Once the risk assessment has been completed (assets and threats-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing. A risk assessment report is a management report that helps senior management make decisions on policy, procedural, budget, system, operational and management changes. This report thus identifies the conditions, tasks and standards that justify various recovery strategies.

Summary

All business processes or systems are not equally critical nor are they equally vulnerable. The objectives of risk assessment is to identify the processes and systems that are at greater risk or more vulnerable so that commensurate efforts are made to strengthen them.

The process of risk assessment starts with the classification of systems into critical, vital, sensitive and non-critical. Once the assets are identified, various threats and threat-sources that may undermine the systems are identified. The next step is to calculate the potential exposure, i.e. the estimated time and cost of disruption and the acceptable downtime. Based on these estimates, the objectives of BCP are formulated.



3 Data Recovery

✂ Learning Goals ✂

To understand:

- ▶ That data is an asset that need to be safeguarded.
- ▶ Various ways of classifying data.
- ▶ Various types of backup.
- ▶ The technical methods available for data backup.

The Information Asset

Electronic data and its storage, more than processors or networks, have become the fulcrum of effective information systems design and integration. Many companies are deploying large scale, stand-alone storage disk arrays or other centralized repository for corporate data including SANs (Storage Area Networks). These centralised storage systems provide heterogeneous platforms to share data seamlessly, usually through high speed networks.

For many businesses, continuity comes down to a simple principle: Reduce the access time to data. For the company experiencing a disruption in a time-sensitive business processes, the critical success factor is to re-establish access to data quickly and by whatever means possible. Companies that take too long to recover key business processes often end up failing completely and disastrously. From an IT standpoint, strategies to reduce the time to data is the key goal of BCP. Once the recovery of data is ensured, the strategies to restore processors, networks and communication links are examined. So, protecting data and assuring its availability for access following a disaster must be the central concern of disaster recovery, for without data, there can be no recovery at all.

Data Classification

To ensure that a data recovery plan is effective, it must ensure that the “right” data is identified and safeguarded against loss. The right data, in this context, refers to data that will be most effective in reducing system failure and increasing the speed of recovery.

This implies that an organisation must have an ongoing identification, classification and protection scheme to keep the data protection plan in synchronization with business priorities. Auditors and managers may

Module 5, Chapter 3

assist in classifying various data elements into the following generic categories:

- ▶ **Critical.** Data or documentation that must be retained for legal reasons, or for use in key business processes, or for restoration of minimum acceptable work levels in the event of a disaster.
- ▶ **Vital.** Data or documentation that must be retained for use in normal business processes and that represents a substantial investment of company resources that may be difficult or impossible to recoup, but may not be required in a disaster recovery situation. Information that requires special secrecy or discretion may also fall under this category.
- ▶ **Sensitive.** Data or documentation that is needed in normal operations, but for which alternative supplies are available in the event of loss. Data that can be reconstructed fairly readily but at some cost, can also be classified as sensitive.
- ▶ **Non-critical.** Data or documentation that can be reconstructed readily at minimal cost, or duplicates of critical, vital, or sensitive data that have no prerequisite security requirements.

Timely recovery is not assured by simply keeping secure offsite data backups. The critical recovery time period requirement means that companies must be able to restore electronic data to an accessible form efficiently so they may be processed by the systems, networks, and end users. How quickly data must be restored to a usable form is determined by the sensitivity of the company to the duration of an un-planned interruption. To address different degrees of sensitivity, several techniques of data backup and restoration have evolved over time. The techniques are discussed below.

Types of Backup

When the backups are taken of data and system files together they are often called “systems backup”, as opposed to a pure data backup. System backups are often either full, incremental or differential.

- ▶ **Full.** A full backup captures all files on the disk or within the folder selected for backup. Because all backed-up files were recorded to a single media or media set, locating a particular file or group of files is simple. However, the time required to perform a full backup can be lengthy. In addition, full backups of files that do not change frequently (such as system files) could lead to excessive, unnecessary media storage requirements.
- ▶ **Incremental.** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. Incremental backups afford more efficient use of storage media, and backup times are reduced. However, to recover a system from an incremental backup, media from different backup operations may be

required. For example, consider a case in which a directory or folder is needed to be recovered. If the last full backup was performed three days prior and one file had changed each day, then the media for the full backup and for each day's incremental backups would be needed to restore the entire directory.

- ▶ **Differential.** A differential backup stores files that were created or modified since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup will save the file each time until the next full backup is completed. The differential backup takes less time to complete than a full backup. Restoring from a differential backup may require less media than an incremental backup because only the full backup media and the last differential media would be needed. As a disadvantage, differential backups take longer to complete than incremental backups because the amount of data since the last full backup increases each day until the next full backup is executed.

A combination of backup operations can be used depending on the system configuration and recovery requirements. For example, a full backup can be conducted on the weekend with differential backups conducted each evening. In developing the system backup schedule, the following factors have to be considered:

- ▶ The place the media will be stored.
- ▶ The data that should be backed up.
- ▶ The frequency of backups.
- ▶ The time required to retrieve backups in the event of an emergency.
- ▶ Authorization for retrieval of the backup media.
- ▶ Personnel who will restore the data from the media.
- ▶ The scheme for media-labelling.
- ▶ Length of time the backup media will be retained.
- ▶ Environmental controls to preserve the media.
- ▶ Choosing the appropriate backup media.
- ▶ The availability of media readers at the alternate site.

Backup media should be stored off-site in a secure, environmentally controlled location. When selecting the off-site location, hours of the location, ease of accessibility to backup media, physical storage limitations, and the contract terms should be taken into account. It is vitally important that media be retrieved on a regular basis from off-site storage and tested to ensure that the backups are being performed correctly.

Technical Methods for Backup

Floppy Diskettes

By default, floppy diskette drives are available with most desktop computers and they are the cheapest backup solution; however, these drives

Module 5, Chapter 3

have a low storage capacity and are slow. They are also the least reliable of all media.

Compact Disk

Compact Disk Read-Only Memory (CD-ROM) drives are a standard peripheral in most desktop computers; however, not all computers are equipped with writable CD drives. CDs are low-cost storage media and have a much higher storage capacity than floppy diskettes. To read from a CD, the operating system's file manager is sufficient; however, to write to a CD, a rewritable CD (CD-RW) drive and the appropriate software is required.

Replication or Synchronization

Data replication or synchronization is a common backup method for portable computers. Handheld computers or laptops may be connected to a PC (Personal Computer) and replicate the desired data from the portable system to the desktop computer and vice versa.

Internet Backup

Internet Backup, or Online Backup, is a commercial service that allows PC users to back up data to a remote location over the Internet for a fee. An utility is installed onto the PC that allows the user to schedule backups, select files and folders to be backed up, and establish an "archiving" scheme to prevent files from being overwritten. Data can be encrypted for transmission; however, this will impede the data transfer speed over a modem connection. The advantage of Internet Backup is that the user is not required to purchase data backup hardware or media.

Removable Cartridges

Removable cartridges are not common in desktop computers and are often offered as a portable or external backup solution. Removable cartridges, are more expensive than floppy diskettes and are comparable in cost to tape media depending on the media model and make. However, removable cartridges are fast, and their portability allows for flexibility. The portable devices come with special drivers and application to facilitate data backups.

Tape Drives

This technique involves regular data backup to magnetic tape using backup/restore software and the transferring of backups to off-site storage. Restoration requires the retrieval of stored backup tapes, transport to system recovery facility, and restoration of data to a new storage platform via software.

This method is the primary data storage and restoration method for the vast majority of the companies that plan for disaster recovery. The disadvantages of this method are that manual transportation and storage

are prone to risk and errors. There is also a considerable long lead time to achieve restoration.

Networked Disk

Data stored on networked PCs can be backed up to a networked disk. A server with data storage capacity is a networked disk. The amount of data that can be backed up from a PC is limited by the network disk storage capacity or disk allocation to the particular user. However, if users are instructed to save files to a networked disk, the networked disk itself should be backed up through the network or server backup program.

Electronic Vaulting and Remote Journaling

Electronic vaulting replaces the manual procedures for handling tape in and out of off-site storage facilities and for transporting tape between locations. A Wide Area Network (WAN) connection is established between the company facility and a remote tape library using some high-bandwidth network interconnection.

Restoration may require the physical retrieval of tapes from the remote tape library and their transport to a systems recovery site, or restoration may be possible using a WAN link between the recovery system and the electronic tape vault. Ideally, in a recovery situation, the company employing electronic tape vaulting should be able to access tape backups immediately from their storage locations at the system backup facility. In some cases, restoration can be initiated and completed by the time recovery personnel arrive at the hot site—representing a significant time savings.

With **REMOTE JOURNALING**, transaction logs or journals are transmitted to a remote location. If the server is to be recovered, the logs or journals could be used to recover transactions, applications, or database changes that occurred after the last server backup. Remote journaling can either be conducted through batches or be communicated continuously using software. Remote journaling and electronic vaulting require a dedicated off-site location to receive the transmissions. The site can be the hot site, off-site storage site, or another suitable location. Depending on the volume and frequency of the data transmissions, remote journaling or electronic vaulting could be conducted over a connection with limited bandwidth.

Remote Mirroring

Remote mirroring is essentially an extension of the concept of internal disk array mirroring. The idea is to perform duplicate writes to disks on identical (or at least similar) disk array platforms located at some distance from the company facility far enough so that the mirrored array is not affected by the same disaster that affects the primary or production array. In some cases, the mirrored array may be located at another

Module 5, Chapter 3

site owned by the organization and remains a component of the organization's internal network. In other cases, the remote mirror may be located at a secure off-site storage facility. In still other cases, the mirror array may be located at a commercial system recovery facility that will be used to recover system platforms in the event of a disaster.

Restoration is unnecessary, since the recovery system is connected via WAN links to the remote mirror array, or because remote mirror may be located at the system recovery site.

Summary

The continuous flow of information is what keeps an organisation functioning. If the flow is disrupted for a length of time, the organisation may not survive. Thus for many organisations the key step in BCP, is ensuring rapid restoration and access to data.

Several technical methods are available for data backup. They range from the floppy diskette which is perhaps suitable for small files to very complex systems such as electronic vaulting, which involves transmitting the backup data to a remote locations, and remote mirroring, which involves concurrent updating of data to the primary site as well as a remote location.



4 System Recovery

✂ Learning Goals ✂

To understand:

- ▶ How and why systems are classified.
- ▶ The strategies available for recovery of different kinds of systems.

Introduction

As with data, systems are also classified based on their criticality. The risk assessment report is the input which provides the management with the data to rank systems according to their criticality. Once the critical systems are identified the management has to decide the recovery strategy. The various options available depend on the type of system, whether centralized, networked or distributed etc.

Contingency Considerations

Nowadays virtually all systems rely extensively on local, telecommunications, and wide area network connectivity. The following actions, which are essentially preventive in nature, help in increasing the speed of recovery or in minimising the impact of a disaster.

- ▶ **Use Results From the Risk Assessment.** Priorities and exposures discovered through the risk assessment of associated LAN, WAN and/or telecommunication systems should be reviewed to determine recovery requirements and priorities.
- ▶ **Standardize Hardware, Software, and Peripherals.** System recovery may be expedited if hardware, software, and peripherals are standardized throughout the system. Recovery costs may be reduced because standard configurations may be designated and resources may be shared. Standardized components also reduce system maintenance across the organization.
- ▶ **Document Systems Configurations and Vendors.** Document the system's architecture and the configurations of its various components. In addition, the contingency plan should identify vendors and model specifications to facilitate rapid equipment replacement after a disruption.
- ▶ **Check Against Security Policies and Security Controls.** Contingency solutions should be checked against network security policies to protect against threats that could compromise network availability. Thus, in choosing the appropriate contingency solutions, security controls and security-related activities (e.g., risk assessment) similar to the

production environment should be implemented in the contingency solutions. This ensures that, during a system disruption, executing the contingency solutions does not compromise or disclose sensitive data.

Strategies for Centralized Systems

The traditional focus of BCP/DRP was the recovery of the corporate computer system, which was almost always a mainframe or large mini-computer. Mainframe-centric disaster recovery plans often concentrated on replacing an inaccessible or non-functional mainframe with compatible hardware. The following are some of the widely adopted strategies for centralized system recovery.

Mirror site/Active Recovery Site

The single most reliable system backup strategy is to have fully redundant systems called an active recovery site or a mirror site. While most companies cannot afford to build and equip two identical data centres, those companies that can afford to do so have the ability to recover from almost any disaster.

In the event of a disaster, redundant systems at a separate facility – which must be far enough so as not to have been affected by the same disaster – are brought on-line. Users are either transported to an operations centre that is co-located to the backup site or are provided remote access to the backup systems through a wide-area data communications network.

This is the most reliable and also the most expensive method of systems recovery.

Hot Site

Hot sites are fully equipped IT operations facilities to which a number of companies having compatible hardware subscribe. It is also possible for a company to have its own dedicated hot site, but it is more usual for a company to have a hot site provided by another commercial organisation.

Machine time is made available to subscribers for the purpose of testing their recovery procedures, and this testing schedule can be quickly interrupted so that facilities can be made available to any customer who declares a disaster. A hot site is usually equipped to run any application that is compatible with its hardware and operating system.

Once a disaster is declared, the affected company sends its backup media (or uses an on-site tape vault or remote mirror) and a team of operations personnel to the hot site. Critical applications are loaded and tested, users are provided with access from their work location, and IT services are restored. If a company requires the use of specialized equip-

ment, the hot site vendor will usually allow it to be installed at the company's expense.

Warm Site

The term warm site is used to describe a facility that is intermediate between a hot site and a cold site, described below. It has all the facilities that are provided by a cold site like raised flooring, air-conditioning, communication links etc. and perhaps other hard-to-get items. But unlike a hot site, the mainframe or the main computer system may not be available. In other cases, a less powerful mainframe or main computer may be installed.

Cold site

A cold site (also known as "shell site") has all the facilities needed to install a mainframe system—raised floors, air conditioning, power, communications lines, and so on. The actual restoration of operations is on hold until replacement hardware can be obtained. By using the cold site strategy, however, the business has already prepared a facility with the requisite physical capabilities to serve as an alternate data processing site.

Company-owned cold sites have the drawback of being expensive to outfit with all of the requisite disaster prevention systems provided in a production data centre. However, the facility may be utilised for other purposes, including off-site storage or new employee training, when not in use for disaster recovery. The alternative to a company-owned cold site is a commercial cold site. A commercial cold site is a contracted facility. The facility may be located in the subscriber's vicinity or away from it. There are also mobile cold sites (see below), where the cold site is actually mounted on a vehicle and can be moved to the customer's location.

Mobile Site

Mobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements. The facility is often contained in a tractor-trailer and may be driven to and set up at the desired alternate location. In most cases, to be a viable recovery solution, mobile sites should be designed in advance with the vendor, and an SLA (Service Level Agreement) should be signed between the two parties. This is necessary because the time required to configure the mobile site can be extensive, and without prior coordination, the time to deliver the mobile site may exceed the allowable downtime of the system.

Reciprocal Agreement

A reciprocal agreement or memorandum of understanding (MoU) is intended to address the problem of break-down of hardware or other

Module 5, Chapter 4

facilities in an organization, which cannot manage its business without information systems for an extended period of time. Two companies, having spare processing time and compatible hardware capabilities, agree formally or informally to back up each other's critical applications. In a simple arrangement, if Company A experienced a disaster, Company B would allow Company A to restore its critical applications on Company B's hardware. The reverse would be the case, if Company B had a failure.

This strategy is no longer very popular. First, it is very difficult for a company to find a partner who had the right hardware, spare capacity, and the inclination to participate in such an agreement. Secondly, since many of these arrangements were informal in nature, changes in system configuration and personnel changes would render this strategy ineffective. This is the cheapest and least reliable strategy for system recovery.

Strategies for Networked Systems

LANs can be implemented in two main architectures:

- ▶ **Peer-to-Peer** — each node has equivalent capabilities and responsibilities. For example, five PCs can be networked through a hub to share data.
- ▶ **Client/Server** — each node on the network is either a client or a server. A client can be a PC or a printer where a client relies on a server for resources.

A LAN's topology, protocol, architecture, and nodes will vary depending on the organization. Thus, contingency solutions for each organization will be different. Listed below are some of the strategies for recovery of LANs.

Eliminating Single Points of Failure

When developing the LAN contingency plan, the organisation should identify single points of failure that affect critical systems or processes outlined in the Risk Assessment. These single points of failures are to be eliminated by providing alternative or redundant equipment.

Redundant Cabling and Devices

Contingency planning should also cover threats to the cabling system, such as cable cuts, electromagnetic and radio frequency interference, and damage resulting from fire, water, and other hazards. As a solution, redundant cables may be installed when appropriate. For example, it might not be cost-effective to install duplicate cables to every desktops. However, it might be cost-effective to install a redundant cable between floors so that hosts on both floors could be reconnected if the primary cable were cut.

Contingency planning also should consider network connecting devices, such as hubs, switches, bridges, and routers.

Remote Access

Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working off-site or allows for a means for servers and devices to communicate between sites. Remote access can be conducted through various methods, including dialup access and virtual private network (VPN). Remote access may serve as an important contingency capability. Recovery teams or users from a distant location can access the corporate data even when they are not in a position to reach the physical premises due to some calamity. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution. Additionally, security controls such as one-time passwords and data encryption should be implemented, if the communication traffic contains sensitive information.

Wireless LANs

Wireless local area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing a wireless network, security controls, such as data encryption, should be implemented, if the sensitive information is to be communicated.

Storage Virtualization

The storage virtualization concept is the process of combining multiple physical storage devices into a logical, virtual storage device that can be centrally managed and is presented to the network applications, operating systems, and users as a single storage pool.

Benefits of storage virtualization are that:

- ▶ storage devices can be added without requiring network downtime,
- ▶ storage volumes from a downed server or a storage device can be re-assigned,
- ▶ assigned storage for a server can be easily created, deleted or expanded to meet the requirements.

Virtualization technologies can complement network-attached storage (NAS) and storage area network (SAN) environments:

- ▶ NAS environments are file-oriented and offer a common storage area for multiple servers. NAS environments are beneficial for file-server applications or storage, such as file sharing or Web and mail services. A NAS device, or server, runs from a minimal operating

Module 5, Chapter 4

system and is designed to facilitate data movement. Using file-oriented protocols, any application residing on any client using virtually any operating system can send data to or receive data from a NAS device.

- ▶ A storage area network (SAN), is a high-speed, high-performance network that enables computers with different operating systems to communicate with one storage device. As opposed to a NAS, a SAN provides data access in blocks and is built to handle storage and backup traffic as opposed to file-oriented traffic. A SAN can be local or remote (within a limited distance) and usually communicates with the server over a fiber channel. The SAN solution moves data storage off the LAN, thus enabling backup data to be streamed to high-speed tape drives, which does not affect network resources as distributed and centralized backup architecture does.

The difference between how a NAS and a SAN function is subtle. A NAS appliance uses an IP protocol to serve files to clients, and a SAN usually uses a fibre channel connection to serve data blocks to servers. A NAS appliance resembles a network server from which clients can obtain files, but a SAN appears as extra storage for each server. NAS appliances send files on request; SANs grant direct access to disks.

RAID

RAID stands for Redundant Array of Inexpensive (or Independent) Disks, a category of disk drives that employ two or more drives in combination. Though off-site storage of backup media enables the system to be recovered, data added to or modified on the server since the previous backup could be lost during a disruption or disaster. To avoid this potential data loss, a backup strategy may need to be complemented by redundancy solutions, such as RAID and load balancing.

RAID provides disk redundancy and fault tolerance for data storage and decreases mean time between failures (MTBF) of systems. RAID is used to insulate the system from disk drive and disk controller failures. In addition, RAID increases performance and reliability by spreading data storage across multiple disk drives, rather than a single disk. RAID can be implemented through hardware or software; in either case, the solution appears to the operating system as a single logical hard drive. With a RAID system, hot swappable drives can be used—that is, disk drives can be swapped without shutting down the system when a disk drive fails. RAID technology uses three data redundancy techniques: mirroring, parity, and striping.

- ▶ **Mirroring.** With this technique, the system writes the data simultaneously to separate hard drives or drive arrays. There are always two drives (or drive arrays) in operation concurrently. The advantages of mirroring are minimal downtime, simple data recovery, and in-

creased performance in reading from the disk. If one hard drive or disk array fails, the system can operate from the working hard drive or disk array; the system can use one disk to process a read request and another disk for a different processing request. The disadvantage of mirroring is that both drives or disk arrays are processing in the writing-to-disks function, which can hinder system performance. Mirroring has a high fault tolerance and can be implemented through a hardware RAID controller or through the operating system.

- ▶ **Parity.** Parity refers to a technique of determining whether data has been lost or overwritten. Parity has a lower fault tolerance than mirroring. The advantage of parity is that data can be protected without having to store a copy of the data, as is required with mirroring.
- ▶ **Striping.** Striping improves the performance of the hardware array controller by distributing data across all the drives. In striping, a data element is broken into multiple pieces, and a piece is distributed to each hard drive. Data transfer performance is increased using striping because the drives may access each data piece simultaneously. Striping can be implemented in bytes or blocks. Byte-level striping breaks the data into bytes and stores the bytes sequentially across the hard drives. Block-level striping breaks the data into a given-size block, and each block is distributed to a disk. Note that striping by itself does not create redundancy. It is only when the each strip of data or block is written to multiple drives that redundancy is created.

Currently, several RAID levels are available, with each level implementing a different configuration.

- ▶ **RAID-0, Striped Disk Array without Fault Tolerance.** RAID-0 is the simplest RAID level, relying solely on striping. RAID-0 has a higher performance in read/write speeds than the other levels, but it does not provide data redundancy and is not fault-tolerant. Thus, RAID-0 is not recommended as a data recovery solution. RAID Level 0 requires a minimum of 2 drives to implement
- ▶ **RAID-1, Mirroring and Duplexing.** RAID-1 uses mirroring to create and store identical copies on two drives. RAID-1 is simple and inexpensive to implement; however, 50 percent of storage space is lost because of data duplication. RAID-1 requires a minimum of 2 drives to implement. The interface to the drives can be through a single controller, which produces the performance of a single drive for reads and writes. Incorporating two controllers (duplexing) can reduce the single-point-of-failure risk. Duplexing can improve I/O data rate by allowing reading from or by writing to both drives simultaneously.
- ▶ **RAID-2, Error-Correcting Coding.** RAID-2 uses bit-level striping; however, the solution is not often employed because the RAID controller is expensive and difficult to implement.

Module 5, Chapter 4

- ▶ **RAID-3, Parallel Transfer with Parity.** RAID-3 uses byte-level striping with dedicated parity. RAID-3 is an effective solution for applications handling large files; however, fault tolerance for the parity information is not provided because that parity data is stored on one drive. RAID-3 requires a minimum of 3 drives to implement.
- ▶ **RAID-4, Dedicated Parity Drive.** RAID-4 is similar to RAID-3, but it uses block-level rather than byte-level striping. The advantage of this technique is that the block size can be changed to meet the application's needs. With RAID-4, the storage space of one disk drive is lost and it requires a minimum of 3 drives to implement.
- ▶ **RAID-5, Block Interleaved Distributed Parity.** RAID-5 uses block-level striping and distributed parity. This solution removes the bottleneck caused by saving parity data to a single disk in RAID-3 and RAID-4. In RAID-5, parity is written across all drives along with the data. Separating the parity information block from the actual data block provides fault tolerance. If one drive fails, the data from the failed drive can be rebuilt from the data stored on the other drives in the array. Additionally, the stripe set can be changed to fit the application's needs. With RAID-5, the storage space of one disk drive is lost. RAID-5 requires a minimum of 3 drives to implement.
- ▶ **RAID-6, Independent Data Disks with Double Parity.** RAID-6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (two-dimensional parity). Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain multiple simultaneous drive failures.
- ▶ **RAID 7.** A very expensive and proprietary (trademark of Storage Computer Corporation) RAID system that adds caching to Levels 3 or 4.
- ▶ **RAID 10.** RAID 10 combines very high reliability combined with high performance. It involves creating multiple RAID 1 mirrors and a RAID 0 stripe is created over these disks. RAID 10 has the same fault tolerance as RAID level 1. It is often referred as RAID 1+0, and requires a minimum of 4 drives to implement.

Generally most organisations use RAID-1 and RAID-5 for data redundancy.

Server Load Balancing

Server load balancing increases server and application availability. Through load balancing, traffic can be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed. With this technique, a group of servers appears as a single server to the network. Load balancing systems monitor each serv-

er to determine the best path to route traffic to increase performance and availability so that one server is not overwhelmed with traffic. Load balancing can be implemented among servers within a site or among servers in different sites. Using load balancing among different sites can enable the application to continue to operate as long as one or more sites remain operational. Thus, load balancing could be a viable contingency measure depending on system availability requirements.

Strategies for Distributed Systems

A distributed system is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server model to make the application more accessible to users in different locations.

Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access, and the elements comprising the distributed system require synchronization and coordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system (DBMS) that supports organisation wide business functions in multiple geographic locations. In this type of application, data is replicated among servers at each location, and users access the system from their local server.

The contingency strategies for distributed system reflect the system's reliance on LAN and WAN availability. Based on this fact, when developing a distributed system contingency strategy, the following methods applicable to system backups should be considered for decentralized systems.

- ▶ Data backups.
- ▶ Electronic vaulting and remote journaling.
- ▶ RAID.
- ▶ Ensuring redundancy of cables and critical system components.
- ▶ Storage Virtualization, NAS or SAN.
- ▶ Remote access.
- ▶ Wireless networks.

In addition, a distributed system should consider WAN communication link redundancy and possibility of using Service Bureaus and Application Service Providers (ASPs).

WAN Communication Link Redundancy

Redundant communications links usually are necessary when the network processes critical data. The redundant links could be of the same capacity or the backup link could provide reduced bandwidth to accommodate only critical transmissions in a contingency situation. For ex-

ample, an ISDN line could be used as a contingency communications link for a primary high speed connection. If redundant links are used, the organisation should ensure that the links have physical separation and do not follow the same path; otherwise, a single incident, such as a cable cut, could disrupt both links.

Service Bureaus/Application Service Providers (ASPs)

Some companies elect to back up systems against failure by contracting with a service bureau for emergency processing services. For example, the vendor of a banking application used by banking companies may offer a “service bureau” capability for the application. If the bank experiences a break-down, the service bureau will undertake to run the application for the benefit of its customers. These kinds of vendor service bureaus are typically application-specific. They may not be suitable for an organisation that has several critical applications from different vendors. Such a company may have to divide various critical applications amongst several vendor provided service bureaus.

An Application Service Provider provides a wider range of services when compared to a vendor-owned service bureau. For example, Oracle Corporation, the database software provider has an ASP service, Oracle Business Online, which offers remote implementation and hosting of Oracle enterprise client/server applications. Quite a few such ASPs are offering a disaster recovery capability as one of the features of such service.

Strategies for Telecommunications Systems

In addition to internal network failures, an organisation has to consider the telecommunication networks also, which links the organisation to the outside world. Some of the options available for recovery of telecommunication systems are given below.

Redundancy

Redundancy involves having extra capacity in order to utilise the surplus capacity whenever the normal or primary telecommunication facility fails. For maintaining the uptime of networks, this strategy could involve the laying of a second cable through a different route. This second cable would be utilised only when the first one is damaged or fails to function.

Alternative Routing

Telecommunications users and providers determined early on that replicating a communications circuit on the same transmission equipment (cable plants, radios, etc.) provided little increase in reliability. Consequently, the practice of replicating high-priority mission critical circuits on alternate paths came into vogue. Alternative routing is de-

sirable since it reduces the likelihood of blocking, it reduces network vulnerability and enhances routing adaptivity to topological and traffic changes. Alternative routing has three main benefits:

- ▶ Routing around failures
- ▶ Routing around congestion, and
- ▶ Optimized routing.

In alternative routing, the information is routed through an alternate medium or path in the event of a disruption. For example, if the primary telecommunication facility is through a coaxial cable, the alternate route could be through twisted pair or fiber optic. This strategy effectively involves the use of different networks, circuits or end points when the primary telecommunication facility is unavailable. In a mesh topology, for instance, several alternate paths exist for the data to move from one node to another. Other examples include dial-up circuits as an alternative to leased lines, cellular phones and radio transceivers as an alternative to land lines and couriers as an alternative to electronic transmissions.

Diverse Routing

A transmission facility path which provides duplicate or backup equipment and geographically separated transmission paths to immediately take over the function of equipment if it fails, or replaces transmission facilities that have been interrupted to prevent communications disruption. Diverse Routing uses circuits serving the same end points but routed over geographically separate transmission facilities. It is a back up cable facility to protect against a single point of failure. An architecture whose security or reliability hinges upon just one mechanism is said to have a single point of failure.

Long Distance Network Diversity

The objective here is to ensure long-distance access, should any one carrier experience a network failure. The disaster recovery team needs to work with the service providers to ensure that redundant lines are not provided through the same physical conduit. It is also important to note that different carriers lease circuits from each other and share the same fiber, conduits, or right-of-way. Many carriers now automatically switch or cutover from one set of trunk links to another set of redundant trunk lines, the moment a failure is detected. The bandwidth on the redundant trunk lines may be lower than that provided by the primary links. A company may still go ahead with its business despite the diminished bandwidth, if fewer end-users utilize applications during the period of outage. The IS auditor should verify the adequacy of connections between company premises, including any recovery site, and the outside world.

“Last Mile” Circuit Protection

The last mile refers to the telecommunication connection from the local exchange to the IS facility. The disaster recovery team also needs to consider how the company will replace mission-critical local loop or the “last mile” network services in the event of the interruption of the service provided by the local telecommunications carrier. One strategy is to secure lines from two different carriers (who use physically separate pathways), also called as “link duplication”. The other strategy, sometimes called “unlike link substitution” is to use different technology or media to achieve link redundancy. For example, ISDN or microwave may be used in an emergency when service through coaxial cable is disrupted.

Voice Recovery

Many business functions are dependent on voice-communications and require line redundancy to ensure that such functions survive a disaster. Planning for recovery of internal communication networks must take into account PBX (Private Branch Exchange) failures. Dedicated lines (i.e., analog or digital lines that do not go through the PBX) may be installed for critical business functions. These lines can be used to handle critical traffic until PBX operations are restored. Also, many PBXs are programmable. Services and capabilities (i.e., call pickup, call forwarding) may be defined as a series of statements. It is important that these programmed instructions are backed up regularly and stored off site together with the documentation for recovery purposes.

Human Resources Issues

Contingency planning is specific to recovery measures for general support systems and major applications; however, such plans are rarely developed or executed on their own. When an incident that impacts IT operations occurs, it often impacts the organization’s personnel. Proper considerations for the safety, security, and well being of personnel should be planned for in anticipation of a disruptive event. Evacuation procedures and regaining access to the facility should be coordinated and jointly exercised with local response organizations and government authorities. Organizations should also have in place methods and procedures for responding to media inquiries. Planning for these factors typically fall within the scope of an Occupant Emergency Plan (OEP), and/or a crisis communications plan, which are all plans coordinated with the business continuity plan.

Personnel Safety and Evacuation

Personnel safety and evacuation during and after a disruption is typically addressed in an OEP. Personnel should be aware of their physical security and exit procedures and should practice these procedures dur-

ing regular fire drill exercises. OEPs and other contingency plans may include instructions for securing office spaces, personal workstations, and laptop computers to prevent access to information and to reduce the likelihood of vandalism or theft. Plans may also include reminders to collect identification badges, car keys, and other important belongings, if the nature of the incident and time allow. Instructions for the most appropriate ways to exit the facility are based on specific site requirements and local fire safety regulations. A “floor warden” methodology may be incorporated into the plan and instituted as a normal practice. This methodology involves designating and training one or two specific people from each floor to be responsible for the evacuation of all personnel. This responsibility usually rotates so that the same people are not responsible for overseeing evacuations throughout the year.

The OEP should also include procedures and multiple contact methods for collecting a personnel headcount after the disaster. It is important for senior management to know who was in the building prior to the event and who has been accounted for (both on- and off-site personnel) so that civil authorities (fire, police, rescue) and families can be properly informed of the situation. Procedures should be developed to instruct personnel to meet and be accounted for at a specific pre-planned site, away from the building. Personnel should be provided alternate procedures to contact the organization. A centralized reporting methodology to one person or to one team will reduce possible confusion and conflicting information.

Personnel Welfare

During a serious situation, addressing personnel and family matters often takes priority over resuming business. Planning for such matters may involve pre-identification of temporary housing, workspace, and staffing. In some situations, the organization may need to use personnel from associated organizations or contract with vendors or consultants if both primary and alternate team members are unavailable or unable to fulfil responsibilities. Preparations should be made during contingency planning development for this possibility to ensure that the vendors or consultants can have the same access as the team members in the event of a disaster. Once personnel are ready to return to work, arrangements should be made for them to work at an alternate site or at home, if the facility is unsafe or unavailable for use. This is an alternate space in addition to the alternate site for contingency operations. Personnel with home computers or laptops should be given instruction, if appropriate, on how to access the organization’s network from home. It may also be necessary to assist personnel with procuring temporary housing.

Disasters may take a heavy psychological toll on personnel, especially if there has been loss of life or extensive physical destruction.

Module 5, Chapter 4

Organizations should be prepared to provide grief counselling and other mental health support. Personnel will be most interested in the status of the health benefits and resumption of payroll. It is very important that the organization communicate this status. Every effort should be made to continue to pay personnel as per normal operations. Due to grief and stress, productivity may also be low during the adjustment period.

Summary

Tolerance of business process is the ability of the organisation to cope with the processes interruption. System are ranked on the basis of their tolerance. Systems that are least tolerant are classified as critical and those with high tolerance are classified as non-critical. Between these two extremes are systems that are classified as sensitive or vital.

There are several steps that an organisation can take in order to expedite the recovery process following a break-down. These include standardization of hardware software and peripherals, documenting configurations and parameters, checking against security policies and controls, and using the results of risk assessment to prioritize systems.

Recovery strategies for centralized systems are relatively straightforward using hot site, cold site, reciprocal arrangements, etc. Recovery of networked systems represent more of a challenge, since the systems are more dispersed and diverse. Many of the technical solutions like storage virtualization, wireless LANs, remote access, etc have become technically and commercially viable only in recent years. Distributed systems represent the greatest challenge, since they are even more dispersed and diverse than networked systems. Redundancy in WAN communication links and Application Service Providers(ASPs) are some of the recovery strategies available for distributed system. Normally telecommunication networks are not owned by the user organisation, therefore recovery strategies for telecom system are limited by the choices offered by telecommunication service providers.

While many organisations have excellent recovery strategies for systems, they often fail to take into account the human factor. Many disasters affect not only systems but also personnel. The organisation must also recognise that following a disaster, most personnel will be far more concerned about their families rather than continuity of businesses. Unless provisions are made for meeting these human needs, a BCP may remain ineffective.



5 Contingency Plan Development

✂ Learning Goals ✂

To understand:

- ▶ The various components of a BCP.
- ▶ The various kinds of plans that are annexed to a BCP.
- ▶ The kinds of risks that can be insured against.
- ▶ How BCPs are tested, validated and maintained.

Components of an Effective Business Continuity Plan

Business continuity plans are created as procedures that describe, or in some cases, prescribe, recovery strategies for various situations. The following sections detail some of the components of a BCP that are common to all types of organisations.

Notification

An event may occur with or without prior notice. For example, advance notice is often given that a cyclone will affect an area or that a computer virus is expected to erupt on a certain date. However, there may be no notice of equipment failure or criminal acts. Notification procedures should be documented in the plan for both types of situation. The procedures should describe the methods used to notify recovery personnel during business and non-business hours. Prompt notification is important for reducing the effects on the IT system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a crash.

Notification Directory

A directory of persons to be notified in the event of a disaster is called a notification directory and is often included in a business continuity plan. The notification directory will include contact information of the following people/organisations:

- ▶ The critical contact persons, who are often the recovery team leaders. These team leaders in turn will call on their team members.
- ▶ Equipment and software vendors.
- ▶ Companies that have been designated to provide supplies and equipment or services.
- ▶ Recovery facilities (including hot site representatives or predefined network communications rerouting services).

Module 5, Chapter 5

- ▶ Off-site media storage facilities and persons within the company who are authorized to retrieve media from the off-site facility.
- ▶ The insurance company.
- ▶ Company providing contract personnel services.

It is also common for a business continuity plan to have a “notification tree” to indicate who will be responsible for calling whom and in what order. Notification trees may also indicate triggers, or chronological points at which a branch of the notification tree is to be notified of some impending activity or event. Communication is essential for command and control of a disaster situation.

Transportation

The organisation also needs to make provisions for the relocation of employees to the user recovery site. This may require establishing a service contract for hiring vehicles at the time of a disaster. In addition to transportation, the company has also to provide for boarding and lodging at the recovery site. Prior to selecting a recovery site which is located too remotely for users to commute from their places of residence, the organisation needs to take an inventory of lodging facilities.

Redirection of Voice Telecommunications Traffic

In many organisations, the loss of voice telecommunications for any period of time effectively results in loss of business functions. Therefore, continuity strategies must account for the recovery of voice telephony capabilities as well. Further voice telephone provides the means for co-ordinating the work of the various recovery teams involved with systems and facility restoration.

Supply Logistics

The organisation must determine what supplies users must have to perform productive work. Some supplies, identified in the risk analysis, may have been stored off-site as part of the off-site backup plan. Arrangements have to be made to ensure that they are retrieved and delivered to the recovery site. A copy of the BCP itself must be stored off-site and copies distributed to key executives to keep at their homes, if necessary. If some supplies (i.e., office supplies) are expected to be acquired from regular sources, the BCP should so state in the recovery plan. Sources and alternates for needed supplies should be specified together with procedures for obtaining them (purchase orders, vouchers, etc.).

Kinds of Plans

There is no universally accepted definitions for contingency planning. This has often led to confusion regarding the actual scope and purpose of various types of plans. To provide a common basis of understanding regarding contingency planning, this section identifies several

other types of plans and describes their purpose and scope relative to a Business Continuity Plan. Because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary from the descriptions below.

Business Continuity Plan (BCP)

The BCP focuses on sustaining an organization's business functions during and after a disruption. An example of a business function may be an organization's payroll process or consumer information process. A BCP may be written for a specific business process or may address all key business processes. IT systems are considered in the BCP in terms of their support to the business processes. In some cases, the BCP may not address long-term recovery of processes and return to normal operations, solely covering interim business continuity requirements. A disaster recovery plan, business resumption plan, and occupant emergency plan may be appended to the BCP. Responsibilities and priorities set in the BCP should match with those in the Continuity of Operations Plan (COOP) to eliminate possible conflicts.

Business Recovery Plan (BRP)

Also called as Business Resumption Plan, it addresses the restoration of business processes after an emergency, but unlike the BCP, lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. Development of the BRP should be based on the disaster recovery plan and BCP. The BRP may be appended to the BCP.

Continuity of Operations Plan (COOP)

The COOP focuses on restoring essential functions of an organization (usually at headquarters) at an alternate site and performing those functions for up to 30 days before returning to normal operations. Because a COOP addresses headquarters-level issues, it is developed and executed independent of the BCP. Standard elements of a COOP include delegation of authority statements, orders of succession, and vital records and databases. Because the COOP emphasizes the recovery of an organization's operational capability at an alternate site, the plan does not necessarily include IT operations. In addition, minor disruptions that do not require relocation to an alternate site are typically not addressed. However, COOP may include the BCP, BRP, and disaster recovery plan as appendices. Note that some organizations use COOP to indicate Continuity of Operations, rather than Continuity of Operations Plan.

IT Contingency Plan

An IT contingency plan should be developed for each major application and general support system. Thus multiple IT contingency plans may be maintained within the organization's BCP.

Crisis Communications Plan

Organizations should prepare their internal and external communications procedures prior to a disaster. A crisis communications plan is often developed by the organization responsible for public communications. The crisis communication plan procedures should be in agreement with all other plans to ensure that only approved statements are released to the public. Plan procedures should be included as an appendix to the BCP. The communications plan typically designates specific individuals as the only authority for answering questions from the public regarding disaster response. It may also include procedures for disseminating status reports to personnel and to the public. Templates for press releases are included in such a plan.

Cyber Incident Response Plan

The Cyber Incident Response Plan establishes procedures to address cyber attacks against an organization's IT system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g., malicious logic, such as a virus, worm, or Trojan horse). This plan may be included among the appendices of the BCP.

Disaster Recovery Plan (DRP)

As suggested by its name, the DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap with that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the organization's needs, several DRPs may be appended to the BCP.

Occupant Emergency Plan (OEP)

The OEP provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Such events would include a fire, hurricane, criminal attack, or a medical emergency. OEPs are developed at the facility level, specific to the geographic location and structural design of the building. The facility OEP may be appended to the BCP.

Insurance

Many organisations choose not to adopt any of the recommended recovery strategy, or if no other reasonable strategy is available, insurances coverage may be used as a strategy to keep the company financially vi-

able. However, insurance is best regarded as a supplement to a properly tested business continuity plan. The following are some of the types of insurance coverage available.

Equipment and Facility Insurance

Property insurance provides cover for loss or damage to property, including IS equipment and facilities. The IS Auditor should review these policies, since under many such policies the insurance company is obligated to replace equipment with “like kind and quality” not necessarily with new equipment by the same vendor as the damaged equipment.

Business Interruption Insurance

Business interruption insurance (also called business income insurance) cover a company’s loss of profits due to a disaster. It also covers continuing expenses that a company is obligated to pay during the time the company is unable to operate.

It is important to note that business interruption insurance is a contingent coverage. It covers consequential loss resulting from a direct loss or damage to property. The coverage is applicable only if a company’s insured property suffers a direct loss. The consequential loss in profit and/or continuing expenses would be covered by business interruption insurance. If there is no direct loss to property, or that loss is not covered by the property policy of the insured, then the business interruption insurance would not apply.

Extra Expense

This is an extremely important add-on to property coverage. Business interruption insurance coverage reimburses an organisation for revenues lost during downtime caused by damage to or loss of property. Extra expense insurance reimburses a company for expenses incurred to avoid or minimize the suspension of business. For example, suppose an IS facility is damaged after a disaster. The business interruption insurance policy pays for the income lost while the IS facility was damaged, whereas, the extra expense policy would cover rent for a temporary office space while the IS facility is being repaired.

Professional Liability (Errors & Omissions) Insurance

Professional liability insurance, also referred to as errors & omissions coverage, is the service equivalent of product liability insurance. It protects the company in the case of a claim against the company for negligence, errors, omissions, or wrongful acts in the performance of the company’s duties. It includes coverage for malpractice, errors, and omissions.

Consultants bidding for corporate contracts are often required to prove that they have errors and omissions coverage, since errors in their work

can put the computer system of the corporation out of commission. It is also a common requirement in government service contracts. The professions for which it is recommended or required include, but are not limited to, computer technicians, systems analysts, accountants, lawyers, and consultants.

Extra Equipment Coverage

If a company's computer equipment is not adequately covered by property insurance, the company can buy a rider or separate policy to cover it. Since IS equipments are also prone to failure due to things like power surges, short circuits, improper grounding, or other forces, the company may need a policy that covers types of equipment breakdowns that are not part of the company's regular property policy.

Data Reconstruction

Ideally the company should go in for insurance that not only covers the physical computer equipment, but also damage to or loss of data. Some insurance companies will write policies that pay for time spent on data reconstruction. However, it should be kept in mind that while insurance companies are willing to underwrite the cost of reconstruction of data lost to a natural or man-made disaster, it would be cost-prohibitive for a company to insure the value of data.

Specialized Equipment Coverage

Special coverage may be available for equipment that does not fit easily into standard coverage or is used in unusual ways. For example, "off-premises" coverage can be applied to expensive equipment such as laptops, network analysis tools, or other items that are used by a company away from its premises. They would be covered in case of off-site theft, loss, or destruction.

Valuable Papers and Records

This covers actual cash value of valuable papers and records on the insured system premises against direct physical loss or damage. This type of insurance pays the cost of recreating documents, re-entering data (including payment for temporary workers) and restoring damaged items.

Fidelity Coverage

This covers the company against loss of corporate assets due to theft, forgery or fraud committed by employees. This type of cover is particularly prevalent among financial institutions.

Civil Authority

These policies cover loss caused by action of civil authority that prohibits access to the premises of the insured. After a disaster, it is possible that the local administration or civil authority may prohibit access to certain areas for safety reasons.

Media Transit

This provides protection in the event that loss, theft or damage occurs during the physical shipment of media. Resulting losses could include service disruption, compromise of data integrity, or privacy.

Continuity Plan Organisation and Implementation

The recovery plan should describe actions to be taken by the organisation to recover and restore the critical applications and their associated resources. It should also spell out the activities to relocate the IT function to a new site or to restore it at the original location. The business plan may include:

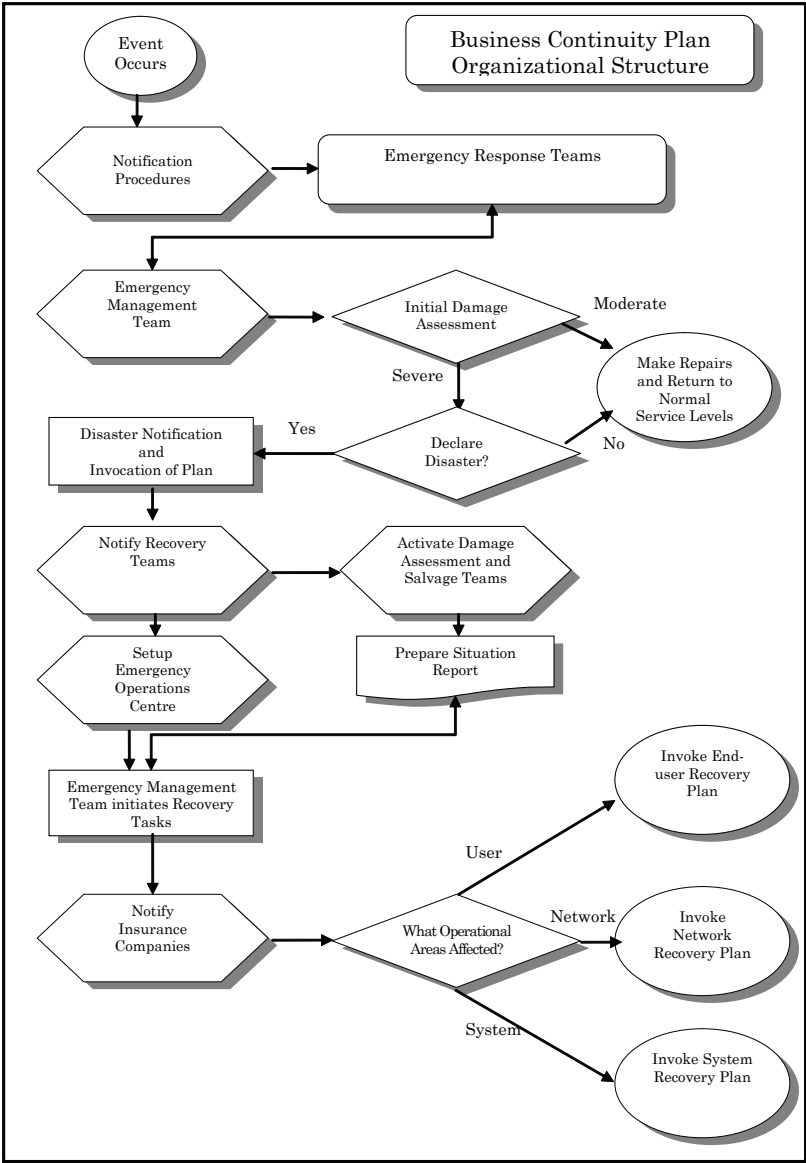
- ▶ **General information.** Organisation, recovery schedule, disaster notification procedures, damage assessment.
- ▶ **Scope.** The scope discusses the issues, situations, and conditions addressed and not addressed in the plan. The section identifies the target system and the locations covered by the contingency plan if the system is distributed among multiple locations. For example, the plan may not address short-term disruptions expected to last fewer than four hours, or it may not address catastrophic events that result in the destruction of the IT facility.
- ▶ **Administrative Procedures.** Corporate communications, role of internal audit, personnel and legal resources, facilities management, insurance information.
- ▶ **Operational Continuity Procedures.** Procedures specific to departments and divisions.
- ▶ **Information Systems Recovery Procedures.** Recovery schedule for hardware, system software, utilities, telecommunications and network, voice and speech circuits.
- ▶ **Application Resumption Plan.** Procedures specific to each application.
- ▶ **Record of Changes.** The contingency plan should be a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to the plan should be recorded in the Record of Changes.
- ▶ **Line of Succession.** The order of succession identifies personnel responsible to assume authority for executing the contingency plan in the event the designated person is unavailable or unable to do so.
- ▶ **Responsibilities.** The Responsibilities section presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms among the teams. The section also provides an overview of roles of team members and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation. Roles should be assigned to team positions rather than to a specific individual. Listing team members by role rather than by name

Module 5, Chapter 5

not only reduces confusion if the member is unavailable to respond but also helps reduce the number of changes that would have to be made to the document because of personnel turnover.

The contingency plan should document technical capabilities designed to support contingency operations. The contingency plan should be tailored to the organization and its requirements. Plans need to balance detail with flexibility; usually the more detailed the plan is, the less scalable and versatile the approach.

The organisation of the business continuity plan may be as per the following diagram.



Testing and Validation

This phase involves the training and testing associated with the validation of the organization’s business continuity plan. Testing a recovery plan must be done on a regular basis to ensure its viability. The auditor should ensure that testing is comprehensive and simulates actual disaster to the extent possible. The testing should also cover manual procedures in addition to information systems.

Module 5, Chapter 5

The plan should be viewed as a dynamic document and needs to be kept current with ever-changing computing and networking requirements. Products and services furnished by the suppliers must also be included in the analysis. The plan will be most effective if it is tested regularly and updated with learning points gathered from each previous test or disaster activation. The plan is only as strong as the weakest facet or component. Testing procedures must include not only the options for redundancy, but must be coordinated with all network and equipment suppliers.

For a test to truly demonstrate the effectiveness of the plan, all units should be tested together. Units that are not used to working together may have to coordinate their efforts during an emergency. It is better to understand and correct coordination problems before an actual emergency is encountered.

There must be a plan for a test. Within the plan there should be a defined test scope and objectives, test scenarios, recovery sequences and test schedules.

The Objectives of Testing

The following are the objectives of testing:

- ▶ **Testing as an audit tool.** Testing is carried out to verify the completeness and accuracy of the business continuity plan. Plan tests are often used to evaluate the efficiency of the plan and to reveal its shortcomings. If the criteria for evaluating test results are properly defined, tests can provide useful information about deficiencies in the plan so that they can be corrected.
- ▶ **Testing as benchmarking.** Plan tests may also reveal useful information about performance of the recovery capability. Certain tests can benchmark how quickly, under optimal conditions, recovery can be reasonably expected to occur following plan activation. Tests also provide information on the actual level of service that is likely to be provided from the alternate site. Other plan provisions and insurance coverage may be reviewed keeping this data in view.
- ▶ **Testing as rehearsal.** Tests also act as training for team members. They provide an opportunity for teams to become familiar with their roles in disaster recovery and how their activities relate to the activities of the other teams. After the test, interviews of the test participants can provide insights into areas that require further review and analysis.

The Phases of Testing

Generally testing goes through three phases, pre-test, test, and post-test.

- ▶ **Pre-Test.** This is a preparatory phase that lays the groundwork for the actual test. It is important to note that activities in this phase will not be carried out during an actual disaster, but only while testing.
- ▶ **Test.** This is the phase where the actual test is carried out. Various operational activities are carried out to test the objectives of the plan. It includes movement of personnel, equipment and supplies to the designated recovery site and execution of various information processing tasks from there. These actions are monitored and evaluated by properly trained and equipped staff members.
- ▶ **Post-Test.** In this phase, all the resources are restored to their original location. This may also include deleting data from third-party systems, restoring equipment and personnel to their normal locations. This phase also comprises the formal evaluation of the plan and suggesting and implementing improvements.

Types of Tests

There are generally five types of tests, listed below in order of increasing comprehensiveness. After a business continuity plan is first drawn up, an organisation goes through each type of test in order. Each test is progressively more complex than the previous and is a more accurate depiction of the actual responsiveness of the company during an actual disaster. The final two types of test involve considerable expenditure of time, effort and resources. The types of tests are:

- ▶ Checklist
- ▶ Structured walk-through
- ▶ Simulation
- ▶ Parallel
- ▶ Full-interruption

Checklist Test

Here copies of the plan are distributed to each of the teams. Each response team should meet to review its response procedures to ensure that all information is current. The plan is then reviewed to ensure that the plan addresses all procedures and critical areas of the organization. Each response team leader should also verify that all team members are aware of their duties and that each team member has copies of the team action plan.

Structured Walk-Through Test

During business continuity plan testing, the response team members should meet to walk-through each step of their resumption procedures. The team should evaluate the effectiveness of each continuation activity and identify gaps, bottlenecks or other weakness in the plan. The objective is to ensure that plan accurately reflects the organization's ability to recover successfully, at least on paper.

Simulation Test

A disruptive event is simulated without impacting normal operations. Among other things a simulation test validates the notification procedures, backup power systems, hardware backup systems, transportation arrangements, alternate communication systems, software and data backup systems, and alternate site processing. The simulation may extend to actually relocating to the backup site and enacting recovery procedures but usually does not involve actual recovery process or alternate processing.

Parallel Test

This is a full test of the plan utilizing all material and human resources. However, normal operations are not interrupted as with the full interruption test described below. Processing is done at both the primary and alternate location. The objective of this type of test is to ensure that critical systems will actually run at the alternate processing backup site as envisaged in the plan. Systems and personnel are relocated and the results of processing at both locations are compared.

Full Interruption Test

This test involves activating the complete business continuity plan and will involve considerable expenditure of time, effort and resources. It includes the mobilization of personnel and resources to an alternate site after interrupting normal operations. The test is recommended for all business operations with critical voice and data processing functions. This test is very costly and should be used and scheduled with extreme caution. It is the most rigorous way to test a business continuity plan.

Documentation of Results

The test should be well documented. Information about the problems that arose during the test and their resolution should be documented. This documentation can be of great assistance during an actual disaster. They are also helpful in improving and maintaining the plan as they reveal the strengths and weaknesses of the plan.

Results Analysis

In order to evaluate the test, there must be some predefined criteria. A typical method used is to produce a set of reports during the live production period and then try to produce exact copies of those reports using back-up equipment, operating systems and data. The test could then be evaluated upon the accuracy of the reports that were run with the back-up resources.

Business Continuity Plan Maintenance

Business continuity plans lose their utility very quickly, often within a year or less, because of changes in staff, vendors and/or resource requirements. Changes in business priorities will result in changes to critical business functions. Functions that were deemed critical when the plan was first formulated may become less critical as the years go by. Technological developments may result in drastic changes to hardware or software environments, which render a plan obsolete. At a minimum, plan reviews should focus on the following elements:

- ▶ Operational requirements
- ▶ Security requirements
- ▶ Technical procedures
- ▶ Hardware, software, and other equipment (types, specifications, and amount)
- ▶ Names and contact information of team members
- ▶ Names and contact information of vendors, including alternate and off-site vendors
- ▶ Alternate and offsite facility requirements
- ▶ Vital records (electronic and hardcopy)

If not maintained, the plan may be ineffective at the time of a disaster and also may have to be written from scratch within a few years. By maintaining the plan on a regular basis, the organisation can avoid this situation.

Summary

A BCP is not merely about systems, it is about people. In any crisis, command and control of the situation is key to its resolution. In a crisis people have to assume responsibilities that are different from their normal day to day tasks. This requires a series of coordinated actions on the part of the personnel involved. The BCP should, therefore, lay down the notification procedure and transportation and other arrangements that will enable effective recovery.

A BCP is rarely a standalone document. It is usually part of a set of documents. There may be an organisation-wide BCP and facility-wise DRP. There may be separate plan, the Cyber Incident Response Plan, to take care of threats like computer viruses and network intrusions. An Occupant Emergency Plan (OEP), may be in use for evacuation of premises during a fire or medical emergencies.

Insurance is yet another tool that supplements a BCP. Monetary losses can be minimised by transferring certain risks to an insurance company on the payment of a premium.

Module 5, Chapter 5

A BCP that exists on paper without being tested serves no useful purpose. The worst possible way to “test” a BCP is to see whether it works during a real disaster. Ideally, while framing the objectives of the BCP, the organisation spells out the “acceptance criteria”, that is, the tests that will validate the BCP. Testing a BCP can be a complex undertaking as many personnel will have to carry out the tests even while continuing with normal operations.



6 Audit and Evaluation of BCP

✂ Learning Goals ✂

To understand:

- ▶ How an IS auditor assesses the adequacy of a BCP.

Audit of BCP

A general review of the Business continuity plan may done along these lines.

Priorities

- ▶ Ensure that the plan's priorities support objectives of the organisation, meet regulatory requirements and conform to contractual requirements.
- ▶ Verify that the plan ensures the survival of the organisation by supporting the timely resumption of information processing capabilities after a disruption.
- ▶ Check for evidence that the priorities have been reviewed and accepted by the appropriate levels of management.
- ▶ Check to see that all applications have been evaluated as to their tolerance for a disruption. Ensure that all critical applications have been identified.

Strategies

- ▶ Verify that the strategies adopted by the company are in line with the priorities.
- ▶ Check for the implementation of the various components of the plan.
- ▶ Check whether the resources allocated for the plan are adequate and whether they will be available within the time frames allowed by the plan.
- ▶ Evaluate the strategy to ensure its adequacy. This includes evaluating any offsite facility and reviewing its security and environmental controls.
- ▶ Determine if the hot-site or other equipment-ready facility has the correct versions of the system software or a compatible version.
- ▶ Review the list of suppliers to be contacted in the event of a disaster to ensure its completeness and appropriateness.
- ▶ Determine whether the plan clearly indicates how movement to the recovery site is to be effected.
- ▶ Examine the adequacy of telecommunications backup.

Module 5, Chapter 6

- Verify that written backup agreements and contracts exist for all facilities, hardware, software, vendors, suppliers, disaster recovery services, and reciprocal agreements. Verify that all agreements are in force and are adequate for the company's needs.
- Evaluate the methods and frequency of data backups and determine their appropriateness.
- Determine the adequacy of offsite data storage.
- Where the company has gone in for a commercial hot or cold site, the IS auditor should obtain a copy of the contract. References provided by the vendor should be verified.
- Evaluate the security of an offsite facility to ensure that it has logical, physical and environmental controls that are commensurate with the risk as assessed during the risk assessment phase. Ideally, these controls should be on par with that provided at the primary facility.
- Determine whether the offsite storage facility has the necessary data files, system software and associated documentation, application software and associated documentation, operations manuals, forms, stationeries, and supplies and a copy of the current business continuity plan. This may require the auditor to perform an inventory review at the offsite facility.

Responsibilities and Tasks

- Ensure that the responsibilities and tasks assigned to various personnel are in accordance with the priorities and strategies.
- Evaluate the ability of IS personnel and other staff to respond effectively in a disaster. This requires a review of emergency procedures, training and results of drills and exercises.
- Ensure that the staff have participated in the development of emergency procedures and assignment of responsibilities and tasks.
- Ensure that the plan is clear and unambiguous.
- Ensure that the current copy of the plan has been distributed.
- Test check contact information (of vendors, employees) to ensure that they are current.
- All key individuals who are critical to the success of the plan should be interviewed. They should demonstrate an understanding of their assigned responsibilities and have an up-to-date documentation of the tasks that are assigned to them.
- Interview a cross section of the employees to ensure that they have understood the responsibilities and tasks assigned to them.
- Ensure there is no excessive dependence on any one person.

Plan Maintenance

- Ensure that a suitable mechanism exists to update the plan.
- The IS auditor should review the results of the business continuity test. The IS auditor should check to see that the results of the test were along anticipated lines. If not, discrepancies between expected

outcomes and actual outcomes should be analyzed to find shortcomings in the plan. The IS auditor should examine whether the weaknesses and shortcomings that have been identified during testing have been rectified at a later date.

Review of insurance coverage

- ▶ The IS auditor should ensure that insurance coverage is adequate and reflects the actual cost of recovery. It is important that the organisation not only cover the loss of property but also cover the loss of revenue stream arising from that property.

Summary

Audit of a BCP is often one of the many points included in an overall audit review, having parity with others such as information security or financial records. The standards (as discussed in the first chapter of this module) form the auditor's toolset for reviewing and reporting on the business continuity. Even in the absence of laws, it may be noted that auditor should review continuity management for the simple reason that he is required to render a true and fair view of the organisation as a "going concern". If the ability of an organisation to survive under adverse circumstances is impaired, the auditor may not be in a position to assume the organisation is a "going concern".



Questions

- Q1. Disaster recovery plan and insurance are:
- A. Controls of first resort.
 - B. Unreliable controls.
 - C. Preventive controls.
 - D. Controls of last resort.
- Q2. The overriding principle behind most continuity plans is
- A. The protection of profits.
 - B. The protection of assets.
 - C. The protection of human life.
 - D. The protection of customers.
- Q3. A comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss is called a:
- A. Business continuity plan (BCP)
 - B. Disaster recovery plan (DRP)
 - C. Disaster continuity plan (DCP)
 - D. Business recovery plan (BRP)

Module 5, Questions

- Q4. The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability is called a/an :
- A. Threat
 - B. Risk
 - C. Exposure
 - D. Hazard
- Q5. Any force or phenomenon that could degrade the availability, integrity or confidentiality of an Information Systems resource, system or network is called a:
- A. Threat
 - B. Risk
 - C. Vulnerability
 - D. Threat-source
- Q6. The correct order of steps for developing a BCP is:
- A. Initiate, Risk assessment, Choose a recovery strategy, Testing and validation, Develop and implement.
 - B. Initiate, Choose a recovery strategy, Risk assessment , Develop and implement, Testing and validation.
 - C. Initiate, Risk assessment, Choose a recovery strategy, Develop and implement, Testing and validation.
 - D. Risk assessment, Initiate, Choose a recovery strategy, Develop and implement, Testing and validation.
- Q7. Enhanced risk awareness and more emphasis on the importance of good risk measurement and management and properly ensured appropriate capital reserve requirements is a requirement of:
- A. Basel Committee's principles for electronic banking
 - B. Basel II Capital Accord
 - C. COBIT
 - D. ISO/IEC 17799:2000
- Q8. A disruption of business operations that stops an organization from providing its critical services caused by the absence of critical resources is called a:
- A. Disaster
 - B. Vulnerability
 - C. Catastrophe
 - D. Calamity
- Q9. Banks must demonstrate that they have an overall data architecture that integrates the various business functions from operations to finance to risk management if they are to achieve compliance with:
- A. ISO/IEC 17799:2000
 - B. SAS 70
 - C. Basel Committee's principles for electronic banking
 - D. Basel II Capital Accord

Module 5, Questions

- Q10. The Generally Accepted System Security Principles (GASSP) is intended to provide authoritative point of reference and legal reference for information security principles, practices, and opinions. These principles were modelled after:
- A. Basel II Capital Accord
 - B. SAS 70
 - C. The Generally Accepted Accounting Principles (GAAP).
 - D. ISO/IEC 17799:2000
- Q11. The order of steps in the process of risk assessment for the purpose of BCP is:
- A. Asset identification and prioritization, Threat identification, Exposure assessment, Objective formulation.
 - B. Objective formulation, Threat identification, Exposure assessment, Asset identification and prioritization.
 - C. Asset identification and prioritization, Exposure assessment, Threat identification, Objective formulation.
 - D. Objective formulation, Asset identification and prioritization, Threat identification, Exposure assessment.
- Q12. The maximum amount of time allowed for the recovery of the of the business function is called the
- A. Maximum Recovery Time Period
 - B. Critical Recovery Time Period
 - C. Minimum Recovery Time Period
 - D. Vital Recovery Time Period
- Q13. Business functions that cannot be done manually under any circumstances are classified as:
- A. Vital
 - B. Essential
 - C. Critical
 - D. Non-critical
- Q14. Within any complex system, there are usually components or processes that, if not replicated or otherwise backed up by redundant capabilities, represent points of failure for the entire system. These are called
- A. Multiple points of failure
 - B. Cascading points of failure
 - C. Linear points of failure
 - D. Single points of failure
- Q15. Business functions that can be performed manually but only for a brief period of time are usually classified as:
- A. Vital
 - B. Essential
 - C. Desirable

Module 5, Questions

- D. Critical
- Q16. Objectives of risk assessment include:
 - A. Sensitizing business processes
 - B. Prioritizing business processes
 - C. Criticising business processes
 - D. Evaluating business processes
- Q17. Risk assessment consists of:
 - A. Data collection
 - B. Data analysis
 - C. Data collection and data analysis
 - D. Data collation
- Q18. During exposure assessment the effects of a disruption may be tracked:
 - A. Over time
 - B. Across related resources and dependent systems
 - C. On the basis of historical costs
 - D. Over time and across related resources and dependent systems
- Q19. Elimination of all risks is usually:
 - A. Impractical or impossible
 - B. Easy to achieve
 - C. Vital to the survival of the company
 - D. Recommended by law
- Q20. Single points of failure are:
 - A. Recommended
 - B. To be eliminated
 - C. Desirable.
 - D. To be encouraged
- Q21. Data or documentation that must be retained for legal reasons, for use in key business processes, or for restoration of minimum acceptable work levels in the event of a disaster is classified as:
 - A. Desirable
 - B. Vital
 - C. Essential
 - D. Critical
- Q22. Data that can be reconstructed fairly readily but at some cost is classified as:
 - A. Critical
 - B. Essential
 - C. Sensitive
 - D. Essential

Module 5, Questions

- Q23. Which of the following media has the least backup capacity?
- A. Removable Cartridges
 - B. Floppy Diskettes
 - C. Compact Disk
 - D. Tape Drives
- Q24. When backups of data and system files are taken together, they are often called:
- A. Systems backup
 - B. Data backup
 - C. Incremental backup
 - D. Differential backup
- Q25. Backup media should be stored:
- A. On-site in a secure, environmentally controlled location
 - B. Off-site in a insecure, environmentally controlled location
 - C. On-site in a insecure, environmentally controlled location
 - D. Off-site in a secure, environmentally controlled location
- Q26. Identify the correct statement:
- A. Both differential and incremental backups take the same amount of time.
 - B. Incremental backups take longer to complete than differential backups
 - C. Differential backups take longer to complete than incremental backups
 - D. Incremental backups take longer when using tape drives.
- Q27. Which of the following is NOT a type of system backup?
- A. Incremental
 - B. Sequential
 - C. Differential
 - D. Full
- Q28. Which of the following technical methods for Backup does not require restoration?
- A. Electronic Vaulting
 - B. Networked Disk
 - C. Tape Drives
 - D. Remote Mirroring
- Q29. A common backup method for portable computers is:
- A. Electronic Vaulting
 - B. Tape Drives
 - C. Remote Mirroring
 - D. Synchronization

Module 5, Questions

- Q30. Which of the following type of system backup would require the maximum storage?
- A. Incremental
 - B. Sequential
 - C. Full
 - D. Differential
- Q31. Which of the following is the MOST reliable strategy for centralized systems?
- A. Cold site
 - B. Reciprocal Agreement
 - C. Hot Site
 - D. Mirror site/Active Recovery Site
- Q32. Which of the following is the LEAST reliable strategy for centralized systems?
- A. Mobile Site
 - B. Hot Site
 - C. Reciprocal Agreement
 - D. Mirror site/Active Recovery Site
- Q33. The process of combining multiple physical storage devices into a logical, virtual storage device that can be centrally managed and is presented to the network applications, operating systems, and users as a single storage pool is called:
- A. RAID
 - B. Storage virtualization
 - C. WAN
 - D. SAN
- Q34. A file-oriented environment that offers a common storage area for multiple servers and which allows any application residing on or any client using virtually any operating system to send data to or receive data is called:
- A. Network-Attached Storage (NAS)
 - B. Remote Access Storage (RAS)
 - C. Redundant Array of Inexpensive Disks (RAID)
 - D. Storage Area Network (SAN)
- Q35. A high-speed, high-performance network that enables different servers with different operating systems to communicate with one storage device is called:
- A. Network-Attached Storage (NAS)
 - B. Remote Access Storage (RAS)
 - C. Redundant Array of Inexpensive Disks (RAID)
 - D. Storage Area Network (SAN)

Module 5, Questions

- Q36. Which of the following is NOT data redundancy techniques used by RAID technology?
- A. Mirroring
 - B. Parity
 - C. Blocking
 - D. Striping
- Q37. Which of the following RAID levels is NOT recommended as a data recovery solution?
- A. RAID-1
 - B. RAID-0
 - C. RAID-10
 - D. RAID-100
- Q38. The technique that allows traffic to be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed is called:
- A. Server Load Balancing
 - B. Alternative Routing
 - C. Diverse Routing
 - D. Storage Area Network
- Q39. Among strategies for telecommunications systems, the strategy that involves the use of different networks, circuits or end points when the primary telecommunication facility is unavailable is called:
- A. Distributed Routing
 - B. Associative Routing
 - C. Diverse Routing
 - D. Alternative Routing
- Q40. Which of the following techniques used by RAID technology increases performance?
- A. Mirroring
 - B. Parity
 - C. Striping
 - D. Hashing
- Q41. A list of persons or organisations to be notified in the event of a disaster and often included in a business continuity plan is called a:
- A. Crisis Communication Directory
 - B. Crisis Communication Plan
 - C. Call Directory
 - D. Notification Directory
- Q42. The plan that addresses the restoration of business processes after an emergency, but which lacks procedures to ensure continuity of critical processes throughout an emergency or disruption is called a:
- A. Business Continuity Plan

Module 5, Questions

- B. Crisis Communication Plan
 - C. Business Resumption Plan
 - D. Continuity of Operations Plan
- Q43. Procedures that are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data, are contained in a:
- A. Continuity of Operations Plan
 - B. Cyber Incident Response Plan
 - C. Crisis Communication Plan
 - D. Business Resumption Plan
- Q44. An IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency is called a:
- A. Disaster Recovery Plan
 - B. Business Resumption Plan
 - C. Continuity of Operations Plan
 - D. Cyber Incident Response Plan
- Q45. The response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property is contained in a/an:
- A. Business Resumption Plan
 - B. Cyber Incident Response Plan
 - C. Business Resumption Plan
 - D. Occupant Emergency Plan
- Q46. With respect to BCP testing, which of the following type of test will involve considerable expenditure of time, effort and resources?
- A. Checklist
 - B. Structured walk-through
 - C. Full-interruption
 - D. Simulation
- Q47. With respect to BCP testing, in which type of test is processing done at both the primary and alternate location?
- A. Full-interruption
 - B. Parallel
 - C. Simulation
 - D. Structured walk-through
- Q48. With respect to BCP testing which is the most rigorous way to test a business continuity plan?
- A. Full-interruption
 - B. Parallel

- C. Simulation
 - D. Structured walk-through
- Q49. Insurance cover that reimburses a company for expenses incurred to avoid or minimize the suspension of business is called:
- A. Business Interruption Insurance
 - B. Equipment and Facility Insurance
 - C. Data Reconstruction
 - D. Extra expense insurance
- Q50. Insurance that protects the company in the case of a claim against the company for negligence, errors, omissions, or wrongful acts in the performance of the company's duties is called:
- A. Business Interruption Insurance
 - B. Equipment and Facility Insurance
 - C. Professional Liability Insurance
 - D. Extra expense insurance
- Q51. Auditor should ensure that the BCP's priorities:
- A. Support objectives of the organisation.
 - B. Meet regulatory requirements.
 - C. Conform to contractual requirements.
 - D. All of the above.
- Q52. Auditor should verify that the recovery strategies adopted by the company are:
- A. In line with audit objectives
 - B. In line with costs
 - C. In line with the priorities
 - D. In line with that of major competitors
- Q53. With respect to a BCP, the auditor should test check contact information (of vendors, employees) to ensure:
- A. They will honour their contractual agreements.
 - B. That they are current.
 - C. They are physically close by.
 - D. They are registered with tax authorities.
- Q54. The auditor should evaluate the security of an offsite facility to ensure that it has logical, physical and environmental controls. Ideally, these controls should be:
- A. On par with that provided at the primary facility.
 - B. Less than that provided at the primary facility.
 - C. More than that provided at the primary facility.
 - D. Different from that provided at the primary facility.

Module 5, Questions

- Q55. The IS auditor should ensure that insurance coverage is adequate and reflects the actual cost of recovery. It is important that the organisation not only covers the loss of property but also:
- A. Covers the health of the employees
 - B. Covers the cost of data reconstruction.
 - C. Covers employee fidelity
 - D. Covers the loss of revenue stream arising from that property.

Answers

QUESTION No	1	2	3	4	5	6	7	8	9	10
ANSWERS	D	C	B	A	D	C	B	A	D	C

QUESTION No	11	12	13	14	15	16	17	18	19	20
ANSWERS	A	B	C	D	A	B	C	D	A	B

QUESTION No	21	22	23	24	25	26	27	28	29	30
ANSWERS	D	C	B	A	D	C	B	D	D	C

QUESTION No	31	32	33	34	35	36	37	38	39	40
ANSWERS	D	C	B	A	D	C	B	A	D	C

QUESTION No	41	42	43	44	45	46	47	48	49	50
ANSWERS	D	C	B	A	D	C	B	A	D	C

QUESTION No	51	52	53	54	55
ANSWERS	D	C	B	A	D

References

Books

- ▶ Information Systems Control and Audit by Ron Weber
- ▶ A Guide to Business Continuity Planning by James C Barnes
- ▶ Auditing Business Continuity, Global Best Practices by Rolf von Roessing
- ▶ The Definitive Guide to Business Resumption Planning Leo A Worbel

Web Resources

- Association of Contingency Planners
- ▶ <http://www.acp-international.com>

Module 5, Questions

Availability.com

- ▶ <http://www.availability.com>

Contingency Planning Management (CPM)

- ▶ <http://www.contingencyplanning.com>

Disaster Recovery Institute International (DRII)

- ▶ <http://www.drii.org>

Disaster Recovery Journal (DRJ)

- ▶ <http://www.drj.com>

The Business Continuity Institute

- ▶ <http://www.TheBCI.org>



Module 6: Information Systems Organisation & Management

1 Information Systems Organization & Management

✂ Learning Goals ✂

This chapter deals with Information systems organization and management. The learning goals of this chapter are:

- ▶ Impact of IT and related competencies and skill-sets
- ▶ Understand importance of Business Process and Enterprise structure
- ▶ Corporate Governance and IT Governance
- ▶ Need and Objectives of IT Steering Committee
- ▶ Objective and methodology of IT Strategy planning
- ▶ Structure of IT enterprise and Relationships
- ▶ Key concepts of IT Policies, Procedures and Practices
- ▶ Concepts of Human Resource management
- ▶ Overview of key IT activities
- ▶ Methodology of Auditing IT policies, procedures and procedures

Key Objectives

The key objectives of this chapter are:

- ▶ To provide overview of the impact of IT and need for related competencies and skill sets.
- ▶ To understand relationship between Business process, Organization structure and controls
- ▶ To understand link between Corporate Governance, principles of IT Governance and IT steering committee.
- ▶ To understand key aspects of IT policies, procedures and practices
- ▶ To understand methodology for Auditing IT policies and procedures.

Impact of IT and the Need for Related Competencies and Skill-sets

The increasing use of Information Technology and increase in the number of large organizations has made it imperative that appropriate information systems are implemented in an organization. The use of IT covering all key aspects of business processes of an enterprise impacts not only how information is processed but also how computerized information systems are used for strategic and competitive advantage. Further, information systems in an enterprise include the internal control system

Module 6, Chapter 1

of an enterprise. Hence, it is important to understand how information systems are organized. The successful design and deployment of information systems determines the success of an enterprise.

The International Federation of Accountants (www.ifac.org) in its guideline on IT competencies and skill sets for Professional accountants highlights that IT is one of the core competencies of professional accountants and requires special attention due to its explosive growth and its rapid rate of change. IT changes have created many new opportunities for professional accountants in areas such as information development and information system design, information system management and control and information system evaluation.

Business Process, Organization Structure and Controls

In an increasingly digitized world, enterprises are using information technology for strategic and competitive advantage and for decision support. Information technology has thus transformed the way business processes are being performed. It is needless to emphasize here that the Information Technology (IT) resources that are deployed are oriented towards achievement of business objectives. The extent of technology deployment also impacts the way internal controls are implemented in an enterprise.

For any IS Audit assignment, IS Auditor will have to understand the business processes of the enterprises, organization structure and related controls. Any enterprise executes its business operations through its staff. Since the organization structure provides the well-defined job responsibilities of each and every employee, an IS Auditor has to understand the organization structure of the enterprise.

Controls

Management Strategy determines at the macro level the path and the methodology of rendering services by an enterprise. Strategy outlines the approach of the enterprise wishes to adopt and is generally formulated by the senior management. Usually, relevant policies and procedures are formulated based on the strategy.

Top management is focused primarily on harnessing the resources of the enterprise towards achievement of business objectives. This would involve the managerial processes of planning, organizing, staffing, directing, coordinating, reporting and budgeting. Control is defined as: Policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented or detected and corrected.

Thus, an IS Auditor could be involved in audits requiring review of Information Systems as implemented or providing consulting before or

during implementation of information systems. In both these cases, understanding of the controls, IS Strategy, policies, procedures, practices and enterprise structure, segregation of duties, etc. are very much essential.

Corporate Governance and IT Governance

Corporate Governance has succeeded in attracting a good deal of public interest because of its importance for the economic health of corporations and the welfare of society. Corporate governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies distribution of rights and responsibilities among different participants in the corporation, such as, the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs.

Corporate governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. It is about doing good business to protect shareholders' interest. Good corporate governance includes sound internal control practices such as segregation of incompatible functions, elimination of conflict of interest, establishment of Audit Committee, risk management and compliance with the relevant laws and standards including corporate disclosure requirements. It is intended to guide companies to achieve their business objectives in a manner that is not done at the expense of shareholders' interest by those who are entrusted with the resources or power to run the companies. Some of the best practices of corporate governance include:

1. Clear assignment of responsibilities for decision-making authorities;
2. Incorporating a hierarchy of required approvals from individuals to the board of Establishment of a mechanism for the interaction and directors; cooperation among the board of directors, senior management and the auditors;
3. Strong internal control systems, including internal and external audit functions, risk management functions independent of business lines, and other checks and balances;
4. Special monitoring of risk exposures where conflicts of interest are likely to be particularly great, including business relationships with borrowers affiliated with the bank, large shareholders, senior management, or key decision-makers within the firm (e.g. traders);
5. The financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition;

Principles of IT Governance

Information Technology (IT) is as an enabler of corporate business strategy. Chief Executive Officers (CEO), Chief Financial Officers (CFO) and Chief Information Officers (CIO) agree that the strategic alignment between IT and business objectives are Critical Success Factors (CSF) for the achievement of business objectives. Corporate governance drives the corporate information needs to meet business objectives. IT should provide critical input to meet the information needs. In other words, corporate activities require information from IT activities in order to meet business objectives. Consequently, corporate governance drives and sets IT governance. The ultimate objective is of course to increase shareholders' value, similar to corporate governance objective. Therefore, there is an inseparable relationship between corporate governance and IT governance.

The IT Governance Institute (www.itgi.org) in its publication: "Board briefing on IT Governance" highlights the importance of IT, IT Governance and the link between enterprise governance and IT Governance. The ITGI publication states that for many organizations, information and the technology that supports it represent the organization's most valuable assets.

IT Governance

IT governance integrates and institutionalizes good (or best) practices of planning and organizing, acquiring and implementing, delivering and supporting, and monitoring IT performance to ensure that the enterprise's information and related technology support its business objectives. IT governance thus enables the enterprise in maximizing benefits, capitalizing on opportunities and gaining competitive advantage.

An important component of IT governance (and by logical extension, corporate governance) is the management and control of risks such as security and reliability of information, besides the realisation of computerisation benefits such as increased organisational effectiveness and efficiency. While IT must be aligned with business objectives, IT governance helps to ensure this by deploying secure, reliable information and technology, the assurance of which is provided by certain controls of the IT activities. The controls should be governed by legal requirements where applicable and generally accepted best practices established by the relevant authorities.

IT Governance and Alignment with Business Objectives

Implementing IT governance effectively requires that IT is implemented as per business needs and IT Governance is aligned with business objectives. Some of the key control objectives to ensure alignment of IT Governance with business objectives are given below:

1. Create an enterprise-wide Information Architecture Model

Information should be kept consistent with needs and should be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities effectively and on a timely basis. Accordingly, the IT function should create and regularly update an information architecture model, encompassing the corporate data model and the associated information systems. The information architecture model should be kept consistent with the IT long-range plan.

2. Create Corporate Data Dictionary and Data Syntax Rules

The IT function should ensure the creation and continuous updating of a corporate data dictionary, which incorporates the organization's data syntax rules.

3. Implement Data Classification Scheme

A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined.

4. Implement and maintain data Security Levels

Management should define, implement and maintain security levels for each of the data classifications identified above the level of "no protection required." These security levels should represent the appropriate (minimum) set of security and control measures for each of the classifications and should be re-evaluated periodically and modified accordingly. Criteria for supporting different levels of security in the extended enterprise should be established to address the needs of evolving e-commerce, mobile computing and telecommuting environments.

IT Steering Committee

In every organization, the roles and responsibilities of the steering committee and its members should be documented and approved by the senior management. The steering committee provides the overall direction for deployment of information technology and information systems in the enterprises. The key functions of the committee would comprise of the following:

- ▶ Ensure that the long and short-range plans of the IT department are in tune with enterprise goals and objectives
- ▶ Establish size and scope of IT function and sets priorities within the scope
- ▶ Review and approve major IT deployment projects in all their stages
- ▶ Approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc
- ▶ Review status of IS plans and budgets and overall IT performance
- ▶ Review and approve standards, policies and procedures

Module 6, Chapter 1

- ▶ Make decisions on all key aspects of IT deployment and implementation
- ▶ Facilitate implementation of IT security within enterprise
- ▶ Facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users
- ▶ Report to board of directors on IT activities on a regular basis

IT Strategy Planning

In any enterprise, there are three levels of managerial activity. They are:

1. Strategic Planning, usually done by the top management
2. Management Control, carried out by the middle management and
3. Operational Control done by first-line managers

Strategic planning is defined as the process of deciding on the overall objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. In the context of Information systems, strategic planning refers to planning undertaken by top management towards meeting long-term IT objectives of the enterprise.

Strategic planning is the process by which top management determines the overall organizational purposes and objectives and how they are to be achieved. Management control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives. Operational control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

A brief overview of IT Strategy planning as per the following classifications is given below:

1. Organization plan
2. Information Systems strategic plan
3. Information systems requirements plan
4. Information systems applications and facilities plan

Organization plan

The organization strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate. It is the primary plan prepared by top management of the enterprise that guides the long run development of the enterprise. It includes a statement of mission, a specification of strategic objectives, an assessment of environmental and organization factors that affect the attainment of these objectives, a statement of strategies for achieving the objectives, a specification of constraints that apply, and a listing of pri-

orities. In a computerized Information Systems environment, it is important to ensure that the IT plan is aligned with the organization plan.

Information Systems Strategic Plan

The Information Systems strategic plan in an enterprise facilitates striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment. This would require the enterprise to have a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals.

COBIT (Control Objectives for Information and Related Technology) is a model of IT Governance and is a collection of best security and control practices. It can be downloaded from <http://www.isaca.org>. COBIT provides some of the enablers of the IS Strategic plan as:

- ▶ Enterprise business strategy
- ▶ Definition of how IT supports the business objectives
- ▶ Inventory of technological solutions and current infrastructure
- ▶ Monitoring the technology markets
- ▶ Timely feasibility studies and reality checks
- ▶ Existing systems assessments
- ▶ Enterprise position on risk, time-to-market, quality
- ▶ Need for senior management buy-in, support and critical review

The Planning and organization domain of COBIT highlights the importance of planning for management of information systems and controls in an enterprise. The key processes in planning domain include defining IT strategic plan, defining information structure, determining technology planning, determine organization structure, etc. The Steering Committee has the responsibility for translating the organization strategic plan into a strategic plan for the information systems function; the steering committee must determine what implications the overall objectives have, for the development of information systems within the enterprise.

Information systems requirements plan

Every enterprise needs to have clearly defined information architecture with the objective of optimising the organization of the information systems. This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information. Based on the information architecture requirements of an enterprise, the IS requirements plan has to be drawn up so as to meet the information requirements of the enterprise. Some of the key enablers of the information architecture are:

- ▶ Automated data repository and dictionary
- ▶ Data syntax rules

Module 6, Chapter 1

- ▶ Data ownership and criticality/security classification
- ▶ An information model representing the business
- ▶ Enterprise information architectural standards

The information system requirements plan defines information system architecture for the information systems department. The architecture specifies the major organization functions needed to support planning, control and operations activities and the data classes associated with each function. The business plan will determine the information needs of an enterprise. The information architecture will determine information needs and flow in an enterprise. This in turn will lead to specific information systems which include the relevant information technology and related processes from the macro to the micro. Readers are advised to refer to Domain 2 (acquisition and implementation) of COBIT for more details.

Information Systems Applications and Facilities Plan

On the basis of the information systems architecture and its associated priorities, the information systems management can develop an information systems applications and facilities plan. This plan includes:

1. Specific application systems to be developed and an associated time schedule
2. Hardware and Software acquisition/development schedule
3. Facilities required
4. Organization changes required

Senior management is responsible for developing and implementing long- and short-range plans that fulfill the enterprise's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the enterprise's long- and short-range plans.

IT Organization and Relationships

Organization structure defines the hierarchy, authority, roles, responsibilities and reporting structure of an enterprise. Organization structure determines the type of job done by each employee type and provides job descriptions. This is the basis for providing authorization and access in information systems to each of the employees. Management should ensure that all personnel in the enterprise have and know their roles and responsibilities in relation to information systems. All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Roles should be designed with consideration to appropriate segregation of duties. No individual staff should control all key aspects of a transaction or event. Everyone should be made aware that they have some degree of responsibility for internal control and security. Management should formally assign the responsibility for assuring

both the logical and physical security of the enterprise's information assets to an information security manager, reporting to the enterprise's senior management. At a minimum, security management responsibility should be established at the enterprise-wide level to deal with overall security issues in an enterprise. If needed, additional security management responsibilities should be assigned at a system-specific level to cope with the related security issues.

Management should create a structure for formally appointing the data owners and custodians. Their roles and responsibilities should be clearly and unambiguously defined. Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and delegate security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures. Senior management should implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised, to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review key performance indicators.

Segregation of Duties

Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are prevented from or monitored for accidental or purposeful errors or omissions or misuse of company assets. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. Moreover, they should ensure that position descriptions for IT staff are established and updated regularly. These position descriptions should clearly delineate both authority and responsibility, include definitions of skills and experience needed in the relevant position, and be suitable for use in performance evaluation.

In particular, a segregation of duties should be maintained between the following functions:

- ▶ Information systems use
- ▶ Data entry
- ▶ Computer operation
- ▶ Network management
- ▶ System administration
- ▶ Systems development and maintenance
- ▶ Change management
- ▶ Security administration
- ▶ Security audit

IT management should undertake the necessary actions to establish and maintain an optimal coordination, communication and liaison structure between the IT function and various other interests inside and outside the IT function (i.e., users, suppliers, security officers, risk managers).

IT Policies, Procedures and Practices

Need for Policies and Standards

Policies are required to provide direction to the staff. They signify the overall plan or course of action adopted and outline the guiding principle to be followed. The senior management sets policies. Based on the policies, appropriate procedures are formulated by the middle management and implemented through the operational management. While formulating the policies, procedures and practices, the internal control system as required by the enterprise has to be given active consideration.

Policies

Policies provide the management guidance and overall direction for effective deployment of Information Resources and its activities. The term policy is also used to refer to the specific security rules for particular systems. Policies are formulated by senior management and represent the strategic philosophy of the enterprise. They should be documented, communicated and reviewed on a periodic basis. Policies should be brief and precise and state the high-level enterprise position and scope. Policies establish who is responsible for compliance with the policy and the corresponding standards.

Procedures

Procedures outline the set of steps to be performed to ensure that a policy guideline is met. They are detailed documents, which help in translation of policies into action plans and guidelines for day-to-day use by business process owners. These include:

- ▶ IT acquisition – Business requirement, Functional Specification, Project Management, RFP issuance, assessment, negotiation and acceptance
- ▶ Help desk
- ▶ User Acceptance Testing
- ▶ Storage, Backup and Managing data
- ▶ Managing facilities
- ▶ Disaster and events Management
- ▶ Change Management
- ▶ Security, patch management, anti-virus vaccine administration, systems usage conditions and rules, etc
- ▶ Managing configuration
- ▶ Hiring, vetting and dismissal procedures

- User procedures and controls
- Operational procedures and controls
- Change categorization, prioritization and emergency procedures
- Escalation procedures

Practices

Practices refer to implementation of policies and procedures for various Information systems and related activities. Practices could be developed for the following areas:

- Practices on Project Management
- Practices on Application Maintenance
- Practices on Data Center Management and Data Processing
- Infrastructure – including servers, storage, networks management
- Human Resources Management refer to enterprise policies and procedures relating to recruitment, retention and termination.
- Outsourcing refers to transfer of processing of data or IT functions to an external entity as terms agreed in a service level agreement also include vendor management
- IT Change Management refers to defined and documented process of managing IT changes in an enterprise.
- Financial management practices refer to all aspects of financial management as related to IT and information systems. This could include IS Budgets,
- Quality Management refers to quality assurance systems and quality control procedures
- Information Security management refers to security policy, procedures and practices
- Performance measures refer to performance management systems relating to IT.

Standards

Standards are established to translate the strategic options into practical and usable user rules and prescribe how specific procedures are going to be performed. They outline the step-by-step approach and methodology so that the specified activities and tasks are performed uniformly as laid down. Standards establish the quality baseline by which activities are measured. There are various international standards covering various areas of IT and IT management. These standards are generic in nature and need to be adapted as per requirements of the enterprise. Enterprises may decide adhering to some international standards in the area of information security. For example, for email security, the organization may select S/MIME as the standard for secure email exchange.

There are many standards related to technology, controls and audit. IS auditors need to have good understanding of IT management standards like ITIL, ISO 15000 and COBIT, security standards like BS 7799 / ISO

Module 6, Chapter 1

17799/ Australian / NZ standards on security, CMM / CMMI standards for Software development. These are covered in Module-7. In addition to these general standards, every enterprise needs to evolve and adapt to standards as relevant for the enterprise. These standards include areas such as vendor selection, procurement of IT infrastructure, installation and maintenance, standard Terms and Conditions, Service Level Agreements (SLAs) etc.

Objectives of the policy

The primary objective of policy is to establish and maintain adequate and appropriate safeguards to ensure confidentiality, integrity and availability of information and related systems. The security policy is designed to protect information by:

- ▶ Denying unauthorized access to any IT resources
- ▶ Restricting access to data or process or any IT resource

Within the operational constraints, the security controls will allow the required services to be available to authorized users only and deny these services to unauthorized users.

IT Policies and Standards

Some of the common policies include:

- ▶ Internet Management Policy
- ▶ Vendor Management Policy
- ▶ IT investment policy
- ▶ Project Management Policy
- ▶ Email Retention Policy
- ▶ Software Management
- ▶ Contracting and Outsourcing
- ▶ Change Management

An IS Auditor is primarily concerned with evaluating

- a. Whether all control procedures are in place;
- b. Identify areas where controls can be impaired; and
- c. Whether policies have been adhered to.

Format of Policy documents

It is advisable to have standard structure and format for developing policy documents. These could include the policy statement, its objective, scope, responsibilities and specific requirements. An example of the format is given below:

Policy Statement

A high-level statement of requirement is needed. For example: “It is the policy of the enterprise that all data communications external to the enterprise will be controlled to prevent unauthorized alteration, destruction or disclosure of data”.

Objective

What the company is trying to accomplish through this policy is stated here. A suitable objective for a data communication security policy could be for example: “To ensure that appropriate cost-effective security mechanisms will be applied to all data communications that use communications networks which are not under the direct control of the enterprise”.

Scope

It is important to communicate how far the policy applies. Taking the above example further, the scope could be defined as: ““This policy applies to all data communications external to the enterprise that will be controlled to prevent unauthorized alteration, destruction or disclosure of data”

Responsibilities

Defining the policy, objective and scope will not ensure its implementation unless clear-cut responsibilities are established for its implementation. Responsibilities are to be specifically defined for:

- ▶ Executive Management
- ▶ Management
- ▶ Information Security Specialists
- ▶ Internal Auditors
- ▶ Information Technology Specialists
- ▶ Information System Users

Specific Requirements

Each policy will have its own specific requirements. Taking the above example further, this could be: “Data traffic will be handled according to the classification level assigned by its owner. These classifications are defined in the Information Classification Policy.” Some more examples relating to specific requirements are:

- ▶ Access to the Internet will only be granted to those individuals who can demonstrate that there is a genuine business need. They will also need to demonstrate the continued usefulness thereof annually.
- ▶ Staff shall not use the Internet or other external connection to download executable programs on to the enterprise's computers. The only exception to this policy statement is where IT staff has a need to use the Internet to obtain technical material for use in relation to approved projects.
- ▶ Staff shall not make unauthorized copies of software and shall use only the licensed software as supplied by the company.

IT Control Policies

Control refers to the policies, procedures, practices and organisation structure designed to provide reasonable assurance that business objec-

Module 6, Chapter 1

tives will be achieved and undesired events will be prevented or detected and corrected. It is important to identify relevant standards relating to Information Systems. For example, the Government of India under the aegis of Ministry of Information Technology has formed the “Centre for IT Security” which provides guidelines and standards relating to security for various IT environments and platforms which can be used and adapted as required for specific audit assignments. (www.mit.gov.in). The control objectives can be translated into specific policy for a specific IT process. While formulating IS Policies, it is important to ensure that the relevant information criteria as identified for audit are considered.

Salient Features of Security Policy

The salient features of Security Policy as per IT Guideline on “Managing Security of Information” issued by International Federation of Accountants are outlined here.

Policy Development

The security objective and core principles provide a framework for the first critical step for any enterprise developing a security policy.

The security policy should support and complement existing organization policies. The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within an enterprise.

The information security policy should describe:

- ▶ The importance of information security to the enterprise;
- ▶ A statement from the chief executive officer in support of the goals and principles of effective information security;

Specific statements indicating minimum standards and compliance requirements for specific areas:

- ▶ Assets classification;
- ▶ Data security;
- ▶ Personnel security;
- ▶ Physical, logical, and environmental security;
- ▶ Communications security;
- ▶ Legal, regulatory, and contractual requirements;
- ▶ System development and maintenance life cycle requirements;
- ▶ Business continuity planning;
- ▶ Security awareness, training, and education;
- ▶ Security breach detection and reporting requirements; and
- ▶ Violation enforcement provisions.
- ▶ Definitions of responsibilities and accountabilities for information security, with appropriate separation of duties;
- ▶ Particular information system or issue specific areas; and
- ▶ Reporting responsibilities and procedures.

Roles and Responsibilities

For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all. Since every enterprise will have its own unique needs, it is not possible to provide a generic approach. Enterprises must assign security related functions in the appropriate manner to nominated employees. Responsibilities to consider include:

- ▶ **Executive Management** – assigned overall responsibility for the security of information
- ▶ **Information Systems Security Professionals** – responsible for the design, implementation, management, and review of the enterprise's security policy, standards, measures, practices, and procedures;
- ▶ **Data Owners** – responsible for determining sensitivity or classification levels of the data as well as maintaining accuracy and integrity of the data resident on the information system;
- ▶ **Process Owners** – responsible for ensuring that appropriate security, consistent with the enterprise's security policy, is embedded in their information systems
- ▶ **Technology providers** – responsible for assisting with the implementation of information security;
- ▶ **Users** – responsible for following the procedures set out in the enterprise's security policy; and
- ▶ **Information Systems Auditors** – responsible for providing independent assurance to management on the appropriateness of the security objectives, and on whether the security policy, standards, measures, practices, and procedures are appropriate and comply with the enterprise's security objectives.

An example of Information Security Policy Statement

Extract from Appendix A of IT Guidelines on Managing Security of Information issued by IFAC is given below. Please note that the purpose of the Information Security Policy is to protect the enterprise's information assets from all types of threats, whether internal or external, deliberate, or accidental. Information systems security is critical to the enterprise's survival.

The Chief Executive Officer supports and has approved the Information Security Policy. It is the Policy of the enterprise to ensure that:

- ▶ Assets will be classified as to the level of protection required;
- ▶ Information will be protected against unauthorized access;
- ▶ Confidentiality of information will be assured;
- ▶ Integrity of information will be maintained;
- ▶ Personnel security requirements will be met;
- ▶ Physical, logical, and environmental security (including communications security) will be maintained;

Module 6, Chapter 1

- Legal, regulatory, and contractual requirements will be met;
- Systems development and maintenance will be performed using a lifecycle methodology;
- Business continuity plans will be produced, maintained, and tested.
- Information security awareness training will be provided to all staff;
- All breaches of information systems security, actual or suspected, will be reported to, and promptly investigated by Information Systems Security;
- Violations of Information Security Policy will result in penalties or sanctions.
- Standards, practices, and procedures will be produced, and measures implemented to support the Information Security Policy. These may include, but are not limited to, virus protection, passwords, and encryption.
- Business requirements for availability of information and information systems will be met.

The roles and responsibilities regarding information security are defined for:

- Executive management;
- Information systems security professionals;
- Data owners;
- Process owners;
- Technology providers;
- Users; and
- Information Systems Auditors

The Information Systems Security function has direct responsibility for maintaining the Information Security Policy and providing guidance and advice on its implementation. All managers are directly responsible for implementing the Information Security Policy within their areas of responsibility, and for adherence by their staff. It is the responsibility of each employee to adhere to the Information Security Policy.

Human Resource Management

There are three key pillars of effective IT deployment: People, Processes and Technology. Processes can be implemented using technology. However, for these to be effective, it is important that people are trained and managed. Hence, people or human resources in an enterprise are most important resource, which have to be managed well to ensure success of technology and processes. This topic has been dealt with in greater detail in a subsequent chapter.

Key IT Activities

The type of job profiles could vary depending on the nature of business, management style, type and extent of IT deployment. However, typically job profiles could be broadly classified as:

- ▶ **Systems Development:** Responsible for development of software
- ▶ **Help Desk/Support:** Responsible for facilitating support to IT users
- ▶ **Operations:** Responsible for all IT and related operations
- ▶ **Librarian:** Responsible for recording, issue, receipt and maintenance of computer files and data
- ▶ **Data entry:** Responsible for data input into the systems done by users or by specified data entry operators
- ▶ **Systems Administration:** Responsible for maintenance of networks, systems and systems software.
- ▶ **Security Administration:** Responsible for maintaining and monitoring security implementation right encompassing policy, standards, procedures and practices
- ▶ **Quality Assurance:** Responsible for implementing Quality assurance systems and quality control procedures
- ▶ **Database Administration:** Responsible for design, definition and maintaining databases, data structures and security of data
- ▶ **System Analysis:** Responsible for designing systems based on user specifications.
- ▶ **System programming:** Responsible for maintaining systems software
- ▶ **Applications Programming:** Responsible for development of new software and maintenance of existing systems
- ▶ **Network Management:** Responsible for maintaining network infrastructure and related components
- ▶ **Project Management**
- ▶ **Data Centre Management**
- ▶ **Customer Relationship Management**

A more detailed description on the nature of roles and responsibilities and controls to be in place is presented in later chapters.

Auditing IT Policies, Procedures and Practices

An IS Audit regardless of its scope and objective would at the macro level, require an overall understanding of the following management aspects of an enterprise:

- ▶ Business processes concerned
- ▶ IT roles and responsibilities defined, including what has been in- or out-sourced
- ▶ Associated business risks and strategic choices
- ▶ Identify the information requirements, which are of particular relevance with respect to the business processes.

Module 6, Chapter 1

- ▶ Identify the inherent IT risks as well as overall level of control, which can be associated with the business process. To achieve this, it is necessary to identify:
- ▶ Recent changes in the business environment having an IT impact
- ▶ Recent changes to the IT environment, new developments, etc
- ▶ Recent incidents relevant to the controls and business environment
- ▶ IT monitoring controls applied by management

The primary objective of an IS Auditor is to review whether control procedures are available and where available, evaluate whether they are operational, adequate and appropriate. Based on this review and evaluation, control weaknesses are identified and the related conditions, causes and effects are highlighted to the management. Hence, to perform an effective IS audit, it is important for the IS Auditor to understand enterprises' policies, procedures and practices.

Based on the review of policies, the standards of the enterprise would be reviewed with the objective of ensuring that all work carried out by the IT department is done in a controlled and standardized manner so that the aims and objectives of the enterprise are met. It is important for the IS Auditor to be acquainted with all relevant standards in order to perform the work adequately. The two basic steps in reviewing the policies and standards:

1. Review the enterprise's policies and standards. All standards must be developed to support the aims of the enterprise expressed in its policies. Thus, the auditor can understand what is required from the computing facilities and establish a benchmark against which to measure when carrying out detailed reviews.
2. Once this benchmark has been established, the auditor should review the enterprise and management of the computer facilities. This allows the auditor to determine if the organization framework exists, within which control can be exercised. It also allows the auditor to establish relationships with management, which can be a great help for future audit reviews.

Audit Procedures for Reviewing Policies

1. Collect all written statements and track them to ensure that they have actually been distributed or are available to all staff. Examine the published organization charts and function descriptions. If these records are not available, then interview the relevant staff to ascertain the adopted practice and verify whether these are documented.
2. Identify the business and IT objectives of the business and to analyse if the IT and related security and control policies support them.
3. Interview senior executives, management and staff at all levels to ensure that they are all comfortable with the requirements.

4. Based on steps 1 to 3 above, decide whether the policies actually add value to the business by making sure that all are following a common direction.
5. Understand why the organization of the IT area is important. Organization allows lines of reporting and responsibility to be defined and allows control systems to be implemented.
6. Examine the organization of the IT department to ensure that adequate division of duties exists, recruitment and staff relations procedures are conducive to control, and training is adequate.
7. Verify whether the documented policies and procedures are actually put into practice as envisaged by the management.
8. Review overall policies and procedures by the operational and managerial staff.
9. Review action taken for implementation of the policies and procedures.

Sample Audit Areas of Policies and Procedures

IS Audit of Policies and procedures encompass all areas of operations of an enterprise. They provide good insight into the enterprise's sense of direction and purpose. Areas of policies and procedures, which could be audited, include but are not limited to:

- ▶ Information architecture
- ▶ IT enterprise and relationships
- ▶ Quality assurance
- ▶ Risk assessment
- ▶ System development life cycle and system documentation
- ▶ System development life cycle methodology
- ▶ Information system security and access
- ▶ Security violation reports and management review procedures
- ▶ Problem management, including recognition, logging, resolution, escalation, tracking and nature management of data
- ▶ Reporting processes
- ▶ Media library and off-site storage of data, etc.

Summary

Business processes enable an organization to achieve business objectives and IT is a key enabler for achieving business objectives. It is important to align IT with business objectives. The objective and functions of steering committee in steering implementation of information systems has been explained. IT Strategy planning process is to be undertaken at regular intervals giving rise to long-range plans and short-range plans. These plans should be translated into operational plans with clear short-term goals. Information systems require an enabling and supporting organization structure to perform key IT activities. Finally, management

Module 6, Chapter 1

of information systems requires appropriate direction, guidance and monitoring by the senior management. This is provided through appropriate IT policies, procedures and practices. This chapter also explains how to audit IT policies, procedures and practices.

References

- ▶ COBIT control objectives IT Process PO1: Define a Strategic IT plan (www.isaca.org)
- ▶ IFAC guidelines on “Managing Security of Information” (www.ifac.org)
- ▶ Chapter 3 of Information Systems control and audit by Ron Weber, 2002 edition, published by Pearson education (Singapore) Pte. Ltd, Indian Branch, Delhi.



2 IT Security and IT Security policies

✂ Learning Goals ✂

This chapter deals with concepts of IT governance and establishes its link with security policy and management issues. The learning goals of this chapter are:

- ▶ IT Regulatory issues
- ▶ IT management needs
- ▶ Need for IT Security
- ▶ How to formulate IT Security Policy
- ▶ Identify key IT Management issues
- ▶ How to Audit IT security and controls

Key Objectives

Regulators have also highlighted the importance of having effective IT regulations in place. This chapter seeks to provide overview of IT security and explains how IT security has to be implemented by senior management through an effective IT security policy. This chapter also focuses on issues of IT management and provides a methodology of auditing IT security and controls.

IT Regulatory Issues

There are numerous changes in IT and its operating environment that emphasize the need to better manage IT-related risks. Dependence on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. Increasing disclosures of information system disasters and increasing electronic fraud, in turn, drive this. The management of IT-related risks is now being understood as a key part of enterprise governance. In the USA, Sarbanes Oxley Act has made it mandatory for a system of internal controls to be implemented and certified by senior management which has to be audited. In India, the RBI issues IT control guidelines to banking sector recommending IT controls to be implemented and also reviews the system of IT related controls and IS Audit in banking. More details on IT Audit and IT guidelines for banking can be obtained from <http://www.rbi.org.in>.

IT Security

Security relates to the protection of valuable assets against loss, disclosure, or damage. In the context of IT, valuable assets includes all IT resources and more so the data or information that is recorded, processed, stored, shared, transmitted, or retrieved in electronic form. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure. The protection is through a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics, firewalls, etc. Security applies to all information. The security concept is summarized in the security objective.

IT Security Policy

IT security policy is defined as the “documentation of measures accepted by the management as necessary to maintain confidentiality, integrity and availability of their information systems”. In arriving at this policy, managers face hard choices involving resource allocation, competing objectives, and organization strategy related to protecting information assets and resources as well as guiding employee behavior. Managers at all levels make choices that can result in policy, with the scope of the policy’s applicability varying according to the scope of the manager’s authority. A security policy is a formal statement on the basis which people are given access to an organization’s resources and information assets.

Security has to encompass managerial, technological and legal aspects. Security policy broadly comprises the following three groups of management:

1. Management members who have budget and policy authority
2. Technical group who know what can and cannot be supported
3. Legal experts who know the legal ramifications of various policy charges

The objective of information security is “the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity.” For any enterprise, the security objective is met when:

- ▶ Information systems are available and usable when required (availability);
- ▶ Data and information are disclosed only to those who have a right to know it (confidentiality); and
- ▶ Data and information are protected against unauthorized modification (integrity).

The relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information system and the business context in which it is used.

An Approach to Implement Security

To meet the security objective and develop and maintain adequate controls in compliance with generally accepted core principles, an ongoing and integrated approach is necessary. The right approach to implementing security would include the following:

- ▶ **Policy Development:** The security objective and core principles provide a framework for the first critical step for any enterprise — developing a security policy.
- ▶ **Roles and Responsibilities:** For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all.
- ▶ **Design:** Once the governing body of the enterprise and related roles and responsibilities assigned has approved a policy, it is necessary to develop a security and control framework that consists of standards, measures, practices, and procedures.
- ▶ **Implementation:** Once the design of the security standards, measures, practices, and procedures has been approved, the solution should be implemented on a timely basis, and then maintained.
- ▶ **Monitoring:** Monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon, and to ensure ongoing compliance with policy, standards, and minimum acceptable security practices.
- ▶ **Awareness, Training, and Education:** Awareness of the need to protect information, training in the skills needed to operate information systems securely, and education in security measures and practices are of critical importance for the success of an enterprise's security program.

The Security policy of an enterprise would broadly cover the following areas:

Access is the ability to do something with a computer resource. This usually refers to a technical ability (e.g., read, create, modify, or delete a file, execute a program, or use an external connection).

Access control is the means by which the ability is explicitly enabled or restricted in some way (usually through physical and system-based controls). Computer-based access controls are called logical access controls. Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted. These controls may be built into the

Module 6, Chapter 2

operating system, may be incorporated into applications programs or major utilities (e.g., database management systems or communications systems), or may be implemented through add-on security packages. Logical access controls may be implemented internally to the computer system being protected or may be implemented in external devices. Logical access controls help protect:

1. Operating systems and other system software from unauthorized modification or manipulation (and thereby help ensure the system's integrity and availability);
2. Integrity and availability of information by restricting the number of users and processes with access; and
3. Confidential information from being disclosed to unauthorized individuals.

Access Criteria: In deciding whether to permit someone to use a system resource logical access controls examine whether the user is authorized for the type of access requested. (Note that this inquiry is usually distinct from the question of whether the user is authorized to use the system at all, which is usually addressed in an identification and authentication process.) The system uses various criteria to determine if a request for access will be granted. They are typically used in some combination. Many of the advantages and complexities involved in implementing and managing access control are related to the different kinds of user accesses supported.

Authorization is the permission to use a computer resource. The application or system owner grants permission, directly or indirectly.

Authentication is proving (to some reasonable degree) that users are who they claim to be.

Identity: The majority of access controls is based upon the identity of the user (either human or process), which is usually obtained through identification and authentication (I&A). The identity is usually unique, to support individual accountability, but can be group identification or can even be anonymous. For example, public information dissemination systems may serve a large group called “researchers” in which the individual researchers are not known.

Roles: Access to information may also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access. Examples of roles include data entry clerk, purchase officer, project leader, programmer, and technical editor. Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. An individual may be authorized for more than one role, but may be required to act in only a single role at a time. Changing roles may require logging out and then in again, or entering a role-changing command. Note that use of roles is not the same as shared-use accounts.

An individual may be assigned a standard set of rights of a shipping department data entry clerk, for example, but the account would still be tied to that individual's identity to allow for auditing.

IT Management Issues

IT Governance Management Guideline requires Governance over information technology and its processes with the business goal of adding value, while balancing risk versus return. While aiming for a reasonable, appropriate and proportional system of controls and safeguards, controls with the highest return on investment (ROI) and those that provide quick wins should receive first priority. The risks and returns of the IT processes are to be defined, balanced and communicated across the enterprise. Key Goal Indicators should be established to ensure improved return on major IT investments.

IT management is a continuous and dynamic process in an enterprise. IT management includes managing issues relating to IT. There are constant pressures due to cost cutting and solutions being evolved. This requires looking at outsourcing; re-look at architecture, merger and acquisition due to IT costs, failed organizations due to inability to invest in IT. An IS Auditor could be involved in a consulting role to suggest specific measures for key areas of IT management. IS auditors in their role as auditors need to look at the process of management of key issues relating to IT. How IT issues are managed determines how successfully an enterprise is able to dynamically adapt to changes and meet the requirements of business. The IT management issues could range from macro issues such as determining the Enterprise information Architecture of the enterprise as is and what is expected to be in the future to meet the present and future needs of the business. This could require identifying problem areas in the present and those, which could arise in the future and identify appropriate solutions. Further, cost-effective management of IT or BPR exercise would demand exploring options of outsourcing and deciding the impact and level of outsourcing. IT Management issues vary from enterprise to enterprise. For example, for a software company where human resources are the most important asset, people retention issues and high attrition rates and their impact on IT management could be an important issue to be managed. There could also be issues, which are common across enterprises such as issues relating to disaster recovery costs and solutions.

Auditing IT security and Controls

The employees in an enterprise perform their job duties with varying degrees of diligence and make judgment calls on items that fall outside established policy and procedure. The execution of delegated instructions tends to deteriorate over time. Management needs a periodic independent check of the execution of policies and procedures, if for nothing

Module 6, Chapter 2

else, to ensure that changes in business conditions have not made the internal control system weak. Auditing IT security and controls would require the following steps:

- Understand clearly the business processes
- Review security policies as documented and implemented
- Review organizational safeguards and controls
- Review defined policies for resources
- Review models and mechanisms to measure security
- Systems Audit
- Ethical hacking
- Availability drills

Some of the areas, which could be audited, include:

- IT mission statement, goals and objectives
- IT Strategy plan, its implementation and monitoring
- IT roadmaps and achievements
- Assessment and management of technology risks
- High level IS security policies
- IT budgets and their variance
- Major IT contracts and Service level agreements
- Systems acquisition, implementation and deployment decisions
- Business continuity plans
- Compliance with IT Regulatory issues

Summary

The need for understanding and implementing IT security and IT security policy has been outlined in this chapter. Certain key issues such as security and security policy have been briefly discussed. Steps for auditing IT security and controls have been discussed.

References

- Board briefing on IT Governance published by IT Governance Institute [<http://www.itgi.org>]
- IFAC guideline on managing security of information. [<http://www.ifac.org>]
- ISACA Guidelines [<http://www.isaca.org>]
- COBIT control objectives [<http://www.isaca.org>]



3 Information Systems Management and Controls

✂ Learning Goals ✂

This chapter deals with Information Systems Management and Controls. The learning goals of this chapter are:

- ▶ Understand Management and Controls
- ▶ Identify Management Responsibility
- ▶ Understand importance of Internal Controls and control objectives
- ▶ How to set IT Control objectives using COBIT
- ▶ Monitoring of Internal Control Systems
- ▶ Categories of Control Techniques: Organization Controls, Management Controls, Financial Control, IT Environment Controls, Physical access controls, Logical Access controls, SDLC controls, BCP controls, Application Controls

Key Objectives

Management is responsible for implementing internal controls in the enterprise. It is the responsibility of the senior management to effectively implement controls as per requirements of the enterprise. This chapter provides examples of IT Control objectives using COBIT. It is not enough to implement controls but the control systems need to be monitored. This chapter also explains different categories of control techniques: Organization Controls, Management Controls, Financial Controls, IT Environment Controls, Physical access controls, Logical Access controls, SDLC controls, BCP controls, Application Controls

Management and Controls

Management is responsible for implementation of the internal control system and auditor is responsible only for the review and expression of an opinion on the internal control system. Control is any action taken by management that would result in accomplishment of the enterprise's goals, objective and mission. Control objectives are management's intentions of what controls should be accomplishing to achieve organizational goals. Internal control refers to any policy, procedure or activity that serves to safeguard assets, maintain accuracy of financial data, improve operational efficiency and enforce adherence to management objectives.

Management Responsibility

Internal Control

Auditing and Assurance standards (AAS) 1, “Basic Principles Governing an Audit” states (paragraphs 18-20): “Management is responsible for maintaining an adequate accounting system incorporating various internal controls to the extent appropriate to the size and nature of the business. The auditor should reasonably assure himself that the accounting system is adequate and that all the accounting information, which should be recorded, has in fact been recorded. Internal controls normally contribute to such assurance. The auditor should gain an understanding of the accounting system and related internal controls and should study and evaluate the operation of those internal controls upon which he wishes to rely in determining the nature, timing and extent of other audit procedures. Where the auditor concludes that he can rely on certain internal controls, his substantive procedures would normally be less extensive than would otherwise be required and may also differ as to their nature and timing.”

The system of internal control is the plan of organization and all the methods and procedures adopted by the management of an entity to assist in achieving management’s objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information. The system of internal control extends beyond those matters, which relate directly to the functions of the accounting system, to all organizational systems, and in particular, to information systems. The internal audit function constitutes a separate component of internal control with the objective of determining whether other internal controls are well designed and properly operated.

The environment in which internal control operates has an impact on the effectiveness of the specific control procedures. A strong control environment, for example, one with tight budgetary controls and an effective internal audit function, can significantly complement specific control procedures. However, a strong environment does not, by itself, ensure the effectiveness of the overall system of internal control. The system of internal control must be under continuing supervision by management to determine that it is functioning as prescribed and is modified as appropriate for changes in conditions. The internal control environment may be affected by:

a. Organizational structure

The organizational structure of an entity serves as a framework for the direction and control of its activities. An effective structure provides for the communication of the delegation of authority and the scope of responsibilities. It should be designed, insofar as practicable, to preclude an individual from overriding the control system and should provide for the segregation of incompatible functions. Functions are incompatible if their combination may permit the commitment or concealment of fraud or error. Functions that typically are segregated are access to assets, authorization of transactions, execution thereof, and record keeping.

b. Management Supervision

Management is responsible for devising and maintaining the system of internal control. In carrying out its supervisory responsibility, management should review the adequacy of internal control on a regular basis to ensure that all significant controls are operating effectively. When an entity has an internal audit system, management may entrust to it some of its supervisory functions, especially with respect to the review of internal control.

c. Personnel

The proper functioning of any system depends on competence and integrity of those operating it. The qualifications, selection and training as well as the personal characteristics of personnel involved are important features in establishing and maintaining a system of internal control.

Categories of Control Techniques

Internal controls can be classified into various categories to illustrate the interaction of various groups in the enterprise and their effect on computer controls. These categories are:

- ▶ Organizational Controls
- ▶ Management Controls
- ▶ Financial Controls
- ▶ Data Processing Environment Controls
- ▶ Physical access Controls
- ▶ Logical access Controls
- ▶ SDLC Controls
- ▶ BCP Controls
- ▶ Application Controls

All these nine categories are briefly described below. Elaborate details on these controls are presented in various other modules.

Organizational Controls

Key Aspects

Although management affects the organization structure and its elements, the owners, shareholders, or board of directors establishes that organization structure; in fact, regulations mandate various aspects of organization structure, including the appointment of an audit committee and direct reporting of the auditor to it. In addition, the regulators require or recommend that the audit department be independent of all other departments and report only to senior management. Regulators require that delegation of any responsibility to lower levels of management be documented in the board meetings minutes.

Enterprise controls are concerned with the decision-making processes that lead to management authorization of transactions. Companies with large data processing facilities separate data processing from business units to provide control over its costly hardware, software, and human resources. Combining data processing into the business units would be too much responsibility for one manager. Organizational control techniques include documentation of:

- ▶ Reporting responsibility and authority of each function,
- ▶ Definition of responsibilities and objectives of each functions,
- ▶ Policies and procedures,
- ▶ Job descriptions, and
- ▶ Segregation of duties.

Responsibilities and objectives

Each IS function must be clearly defined and documented, including systems software, application programming and systems development, database administration, and operations. The senior manager, of all these groups, and managers of the individual groups make up the IS management team responsible for the effective and efficient utilization of IS resources. Their responsibilities include:

- ▶ Providing information to senior management on the IS resources, to enable senior management to meet strategic objectives.
- ▶ Planning for expansion of IS resources
- ▶ Controlling the use of IS resources
- ▶ Implementing activities and functions that support accomplishment of company's strategic plan.

Policies, standards, procedures and practices

These are the standards and instructions that all IS personnel must follow when completing their assigned duties. Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. Procedures establish the instructions that individuals must follow to complete their daily assigned tasks. Mandating that all requests for changes to existing programs must be approved by user and IS management before programmers and analyst can work on them is an example

of a policy. Documented instructions for filling out a standard change request form, how to justify the costs of the change, how to specify the changes needed, how to obtain approvals, and who to obtain the approvals from are examples of procedures. Documented policies should exist in IS for:

- ▶ Use of IS resources,
- ▶ Physical security,
- ▶ Data security
- ▶ On-line security,
- ▶ Microcomputer use,
- ▶ Reviewing, evaluating, and purchasing hardware and software,
- ▶ System development methodology, and
- ▶ Application program changes.

Documented procedures should exist for all data processing activities. These procedures will be expanded upon in the chapters on individual audit areas.

Job descriptions

These communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee. All jobs must have a current, documented job description readily available to the employee. Job descriptions establish responsibility and the accountability of the employee's actions.

Segregation of duties

This is a common control technique aimed at separating conflicting job duties, primarily to discourage fraud, because separating duties makes collusion necessary to commit a fraud. Such separation can also force an accuracy check of one-person work by another, so that employees to some extent police each other. Examples of segregation of duties are:

- ▶ Systems software programming group from the application programming group
- ▶ Database administration group from other data processing activities
- ▶ Computer hardware operations from the other groups
- ▶ Application programming group into various subgroups for individual application systems
- ▶ Systems analyst function from the programming function
- ▶ Physical, data, and online security group(s) from the other IS functions.
- ▶ IS Audit

It is the responsibility of the senior management to implement a division of roles and responsibilities, which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipu-

Module 6, Chapter 3

lated for their respective jobs and positions. From a functional perspective, segregation of duties should be maintained between the following functions:

- ▶ Information systems use
- ▶ Data entry
- ▶ Computer operation
- ▶ Network management
- ▶ System administration
- ▶ Systems development and maintenance
- ▶ Change management
- ▶ Security administration
- ▶ Security audit

Management Controls

These controls are concerned with long-range planning, legal compliance, and resource usage. Planning includes goals and objectives covering at least the next five years, and short-range goals, objectives, functions and activities needed to meet those long-range goals.

Resource usage refers to the planning and allocation of all assets, including buildings, furniture, computer hardware, application, facilities and data- like diagrams, documentation, software licenses, and contracts. The management controls should be linked to policy and are to be monitored to ensure that appropriate standards are prescribed and practiced. The number of management levels depends on the company size and organization structure, but generally, there are three such levels senior, middle, and supervisory. Senior management is responsible for strategic planning and objectives thus setting the course for the lines of business that the company will pursue. Middle management develops the tactical plans, activities, and functions that accomplish the strategic objectives, supervisory management oversees and controls the daily activities and functions of the tactical plan.

Long-range planning

The long-range planning process should be quite exhaustive, covering every department, and it must be updated yearly to adjust the elements delineated above. Good long-range planning includes documenting goals and objectives, explaining how strengths will be used, and how weakness will be compensated for or corrected. Time allowances, target dates, revenues, and expenses are estimated and documented for use in standards for progress measurement. The elements of long-range planning incorporate:

- ▶ The goals and objective of the plan-for use in measuring progress,
- ▶ Revenue and expense estimates,
- ▶ Time allowance and target dates, and
- ▶ Strengths and weaknesses.

Long-range planning and IT department

COBIT IT Process 1 of Planning and Organization Domain : Define IT strategic planning outlines senior management's responsibility for developing and implementing long- and short-range plans that fulfill the organization's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organization's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organization. The IT department must inform senior management of its strengths and weaknesses, isolating and describing the support that can be given using existing resources to achieve the stated goals and objectives. With proper long-range planning, these deficiencies should become known early enough for the company to react and correct the deficiency in time.

Short-range planning or tactical planning

This refers to the establishment and documentation of goals, objectives, functions, and activities needed to meet all of the elements of the long-range plan. The functions and activities are performed every day, whereas the tactical goals and objectives define deliverables (final products) that span periods of time as close as tomorrow and as far away as five years. For data processing, the short-range plan defines the daily activities of developing software and obtaining hardware in sufficient time to support business activities.

As part of planning process, enterprise needs for complying with the external requirements to meet legal, regulatory and contractual obligations have to be carefully considered. For example, the Information Technology Act, 2000 enforces the need for the management to ensure due diligence in various areas of IT management. Further, banks are subject to detailed guidelines pertaining to provision and sharing of information. It is important to identify and analyse external requirements for their IT impact, and taking appropriate measures to comply with them. This means that for many companies, ensuring that all statutes are adhered to can be a daily activity. IT must be constantly aware of the changing legal environment that affects the department's business.

Personnel management controls

This involves activities and functions to accomplish the administration of individuals, salary, and benefits costs. The control techniques are:

- ▶ Job descriptions,
- ▶ Salary and benefits budget,
- ▶ Recruiting standards and criteria,
- ▶ Training and development programs,
- ▶ Job performance evaluations, and

Module 6, Chapter 3

- ▶ Screening and security standards.

Job descriptions: These are also organizational controls. They also function as a management control from the standpoint that they communicate management requirement to the employee and provide a standard for performance measurement.

Salary and benefit budgets: these help management control these costs and plan for the future. New product and services must be sold and supported by people. These costs must be known when pricing a product or service, the strategic and tactical plans should identify these cost factors since they can make or break the offering of a new service or product,

Recruiting standards and criteria: these are particularly applicable to technical training and experience requirements needed for IS positions. The pool of available personnel could be thin if the company uses unique or unusual hardware and software that demands specialized training and development programs to obtain the proper staff. Programs that support IS are IS management's responsibility, largely because the personnel department may not be able to develop and maintain technical IS training courses.

Job performance evaluations: These are needed to counsel and motivate employees who are measured against their job descriptions and other performance criteria. In data processing, job performance evaluations should consider the quality of the designed and written programs, the conformance with deadlines and budgeted time, and compliance with data processing standards.

Screening and security checks: these have unique applicability to data processing because program design is a pervasive activity that can have a profound effect on the entire company. Programs that are fraudulent or intentionally erroneous can damage a company, even causing bankruptcy. Thorough screening of the prospective employee, obtained by talking with previous employers and obtaining credit reports, is one preventive control against fraud and sabotage, applicable labour laws and regulations, however, affect the extent of screening an employer can perform.

Financial Control Techniques

These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. The

financial control techniques are numerous. A few examples are highlighted here:

Authorization: This entails obtaining the authority to perform some act, typically access to such assets as accounting or application entries.

Budgets: These estimates of the amount of time or money expected to be spent during a particular period of time, project, or event. The budget alone is not an effective control—budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.

Cancellation of documents: This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a “paid” or “processed” stamp or punching a hole in the document.

Documentation: This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.

Dual control: This entails having two people simultaneously access an asset. For example, the depositories of banks’ 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.

Input/output verification: this entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.

Safekeeping: this entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.

Segregation of duties: this entails assigning similar functions to separate people to provide reasonable assurance against fraud and provide an accuracy check of the other persons work. For example, the responsibilities for making financial entries to the application and to the general ledger should be separated.

Sequentially numbered documents: These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

Module 6, Chapter 3

Supervisory review: This refers to review of specific work by a supervisor: but what is not obvious is that this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

Transmittal documents: this is a piece of paper describing the contents of the items attached to it or sent separately, a type of cover letter. It provides a double check of the processing accuracy of the documents or items represented by the transmittal document. It typically includes a brief description of the items sent, dollar totals of all items in the group, and an item count, the documents tells the receiving area what items should be attached.

Data Processing Environment Controls

These controls are hardware and software related and include procedures exercised in the IS environmental areas. The environmental areas include system software programming, on-line programming, on-line transaction systems, database administration, media library, application program change control, the data center and the media library.

Physical Access Controls

These controls are personnel; hardware and software related and include procedures exercised on access by employees/outside to IT resources. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy. These Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to individuals who have been authorized to gain such access. Where IT resources are located in public areas, they should be appropriately protected to prevent or deter loss or damage from theft or vandalism. Further, IT management should ensure a low profile is kept and the physical identification of the site of the IT operations is limited. The other measures relate to Visitor Escort, Personnel Health and Safety, Protection against Environmental Factors and Uninterruptible Power Supply.

Logical Access Controls

These controls are software related and include procedures exercised in the IS software through access controls through system software and application software. Logical access controls are implemented to ensure

that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and access control, user identification and authorization profiles, incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

SDLC (System Development Life Cycle) controls

These are functions and activities generally performed manually that control the development of application systems, either through in-house design and programming or package purchase. The first control requirement is system development standards that specify the activities that should occur in each system development life cycle (SDLC) phase. For example, these standards specify the type and quantity of testing that should be conducted. The second element of controls is documented procedures communicate how the activities in each phase should be accomplished. These procedures establish control functions in each phase

Business Continuity (BCP) Controls

These controls relate to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption. The controls include criticality classification, alternative procedures, back-up and recovery, systematic and regular testing and training, monitoring and escalation processes, internal and external organizational responsibilities, business continuity activation, fallback and resumption plans, risk management activities, assessment of single points of failure and problem management

Application Control Techniques

These include the programmatic routines within the application program code. The financial controls, discussed earlier, are performed by the user to help ensure the accuracy of application formed by the use to help ensure the accuracy of application processing. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, data ownership, data administration policies, data models and data representation standards, integration and consistency across platforms, legal and regulatory requirements. Any function or activity that works to ensure

Module 6, Chapter 3

the processing accuracy of the application can be considered an application control.

Summary

This chapter has highlighted the importance of IS management and controls in an enterprise. Implementation of Information technology brings with its inherent risks. These risks need to be mitigated by implementing an appropriate system of control framework. Management is responsible for implementing this control framework. The internal control system should have internal controls, which meet control objectives. Finally, different types of control techniques relating to all key aspects of information technology deployment have been discussed.

References

- ▶ Auditing and Assurance Standards of ICAI [<http://www.icaai.org>]
- ▶ Chapter 3 of Information Systems control and audit by Mr. Ron Weber, 2002 edition, published by Pearson education (Singapore) Pte. Ltd, Indian Branch, Delhi



4 IS Management Practices

✂ Learning Goals ✂

This chapter provides an overview of IS Management Practices. The learning goals are:

- ▶ Understand key aspects of Human resource Management
- ▶ Identify and evaluate Performance Management measures
- ▶ Evaluating User satisfaction
- ▶ Understand documentation Standards
- ▶ How to Benchmark existing practices
- ▶ Overview of ISO standards
- ▶ How to Audit IT Management practices

Key Objectives

Management controls include the system of policies, procedures and practices as implemented in an organization. Management practices are the final translation and effect of how overall management policies are actually implemented. Policies are high level documents and procedures are detailed documents. However, what is actually practiced and implemented is referred to as practices. Practices need to encompass all key aspects of management in an enterprise to ensure that policies, standards and procedures are effectively implemented. This chapter deals with some of the key information systems management practices such as Human Resource Management, Performance Management, User Satisfaction and Documentation Standards. Further, this chapter also provides an overall understanding of benchmarking and steps to perform benchmarking exercise. An overview of history and type of ISO standards as relevant to information systems is provided. Finally, a simple step-by-step approach for auditing IT management is explained in this chapter.

Human Resource Management

Information security management involves each and every person who interacts with information. Every person has the capability of sabotaging the information security either because of ignorance or malicious intent. Training should explain each individual's role in maintaining the information security and his/her responsibilities towards every information asset that he/she handles. Training should be comprehensive and adequate to ensure that each person clearly understands the security policies of the organization, various security risks and threats and finally consequences of not abiding by the security procedures. It is es-

Module 6, Chapter 4

essential that the following resource elements have a systematic management process in place:

- ▶ Human resources;
- ▶ Recruitment procedures;
- ▶ Reporting requirements and procedures;

Of these, management procedures dealing with human resources, equipment and software are the most relevant to the deployment of information and communications technology. Key sets of issues, related to the overall planning for the deployment of resources, have emerged as particularly important to business practice. These issues are also particularly difficult to handle. In the context of IT, these issues, or strategic organizational requirements, include:

- ▶ Development of a strategy for IT systems implementation;
- ▶ Management of IT and communications resources;
- ▶ Management of information security;
- ▶ Human resource planning for delivery of the IT strategy;
- ▶ Management of the resource planning process; and
- ▶ Software implementation for control of resource planning.

Best Practices on HR Management

Human resources are the most critical resource of an enterprise that ensures that the goals and objectives of the enterprise are achieved. Compared to the risks of the three key resources people, process and technology, it is people who can facilitate or impair effective implementation of technology and processes. It is important for senior management to have a proper system of HR management and implement best practices as feasible. Given below are outline of some of the best practices and brief explanation of some of the key HR practices.

- ▶ Implement and regularly assess the needed processes to ensure that personnel recruiting and promotion practices are based on objective criteria and consider education, experience and responsibility.
- ▶ Ensure that these processes are in line with the overall enterprise's policies and procedures in this regard, such as hiring, orienting, training, evaluating, counselling, promoting, compensating and disciplining.
- ▶ Assess knowledge and skill needs on a continuous basis so that employees have skills, which match those necessary to achieve enterprise goals.
- ▶ Regularly verify that personnel performing specific tasks are qualified on the basis of appropriate education, training and/or experience, as required.
- ▶ Encourage personnel to obtain membership in professional enterprises.

- Clearly define roles and responsibilities for personnel, including the requirement to adhere to management policies and procedures, the code of ethics and professional practices.
- Ensure that terms and conditions of employment stress the employee's responsibility for information security and internal control.
- Provide employees with orientation upon hiring and with on-going training to maintain their knowledge, skills, abilities and security awareness to the level required to perform effectively. Education and training programs are to be conducted to effectively raise the technical and management skill levels of personnel and are to be reviewed regularly.
- Provide for sufficient cross training or back up of identified key personnel
- Establish succession plans for all key functions and positions.
- Ensure that personnel in sensitive positions are required to take uninterrupted holidays of sufficient length to exercise the enterprise's ability to cope with unavailability and to prevent and detect fraudulent activity.
- Ensure that personnel are subjected to security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position.
- Implement an employee performance evaluation process, reinforced by an effective reward system that is designed to help employees understand the connection between their performance and the enterprise's success.
- Ensure that such evaluation is performed against established standards and specific job responsibilities on a regular basis.
- Ensure that appropriate and timely actions are taken regarding job changes and job terminations so that internal controls and security are not impaired by such occurrences.

Hiring

Clearances must be obtained for persons in sensitive positions. It is the responsibility of the management to ensure that IT related positions meet the security guidelines established by the enterprise and that all information systems-related positions requiring sensitive clearances are identified and that clearances are kept current. To hire the right person for a job, it is important that both management and the applicant for the job understand clearly the requirements of the job. For each position, a formal documented job specification must exist defining the nature of the job, its duties and opportunities for advancement. The job specification forms the basis of advertising the job and evaluating applicants for the job.

Personnel can be recruited internally or externally to the enterprise. Internal recruitment enhances morale and captures existing experience

Module 6, Chapter 4

within the enterprise. External recruitment may result in a better match between the job specification and the applicant's skill set. It also injects new knowledge into the enterprise.

Management must obtain data to evaluate applicants through interviews, aptitude tests, references, resumes and scholastic records. Some basic control procedures that should be applied include:

- ▶ Background checking of references, resumes, scholastic records, etc.
- ▶ Screening applicants for mental and physical health
- ▶ Bonding of key employees
- ▶ Explanation of enterprise protocol to be observed, example: matters not to be discussed in public.
- ▶ General enterprise indoctrination – example: matters covering key aspects of enterprise

Control risks are:

- ▶ Staff may not be suitable for the position they are recruited for.
- ▶ Reference checks are not carried out
- ▶ Temporary staff and third-party contractors may introduce uncontrolled risks.

Promotion Policies

Promotion Policies encourage employees and boosts their morale. Hence, it should be fair and comprehensive to employees. Policies should be based on objective criteria and should consider an individual's performance, education, experience and level of responsibility.

Training

Training must not be haphazard. It should be given on a fair and regular basis to all employees. Those areas where employees lack expertise should be identified. Proposed coursework should be carefully evaluated. This is particularly important when new hardware and software are being implemented. Training should include relevant management training, project management and technical training.

Scheduling and Time Reporting

Proper scheduling provides for efficient operation and use of computing resources. Time reporting allows management to monitor the scheduling process as per the time schedule. Management can then determine if staffing is adequate and if the operation is running efficiently. It is important that the information being entered or recorded into such a system is accurate.

Employee Performance Evaluations

With the regular use of standard employee performance evaluations an enterprise can assess employees. This tool can assist in identifying promotional candidates and compare salaries to others in the same indus-

try. Performance evaluations also can be used to gauge employee satisfaction.

Required Vacations

A required vacation (holiday) ensures that once a year, at a minimum, someone other than regular employees will perform a job function. This reduces the opportunity to commit a fraud. During this time it may be possible to discover fraudulent activity as long as there has been no collusion between employees to cover possible discrepancies. Job rotation provides an additional control (to reduce the risk of fraudulent or malicious acts), as the same individual does not perform the same task all the time. This provides an opportunity for an individual other than the regularly assigned person to perform the job and notice possible irregularities.

Termination Policies

Personnel termination may be voluntary or involuntary. In either case, certain control procedures should be exercised. Written termination policies should be established to provide clearly defined steps for employee separation. It is important that policies be structured to provide adequate protection for the enterprise's computer assets and data. Termination practices should address:

- ▶ Voluntary termination
- ▶ Immediate termination
- ▶ Return of all access keys, ID cards, smart cards and badges to prevent easy physical access.
- ▶ Notification of fellow employees to increase awareness of the terminated employee's status.
- ▶ Deletion of assigned logon-ID and passwords immediately to prohibit system access.
- ▶ Arrangement of the final pay routines to remove the employee from active payroll files.
- ▶ Performance of a termination interview to gather insight on the employee's perception of management.
- ▶ Return of all company property
- ▶ Escort from the premises.

Employee Handbook

Employee handbooks, generally distributed to all employees upon being hired, could cover:

- ▶ Security policies and procedures
- ▶ Company exceptions
- ▶ Employee benefits
- ▶ Vacation (holiday) policies
- ▶ Overtime rules
- ▶ Outside employment

Module 6, Chapter 4

- ▶ Performance evaluations
- ▶ Emergency procedures
- ▶ Disciplinary actions for excessive absence, breach of confidentiality and/or security, non-compliance with policies

In general, there should be a published code of conduct for the enterprise that specifies all employees' responsibilities to the company.

Performance Management

COBIT Control Objectives in Domain 3 (delivery and support) Manage Performance and Capacity provides control objectives for performance management. It outlines the best practices to be adopted by an enterprise. Some of key best practices to be adopted are:

- ▶ Management process should ensure that business needs are identified regarding availability and performance of information services and converted into availability terms and requirements.
- ▶ Establish availability plan to achieve, monitor and control the availability of information services.
- ▶ Implement a process to ensure that the performance of IT resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.
- ▶ IT management should ensure that appropriate modeling tools are used to produce a model of the current system which has been calibrated and adjusted against actual workload and is accurate within recommended load levels.
- ▶ Modeling tools should be used to assist with the prediction of capacity, configuration reliability, performance and availability requirements. In-depth technical investigations should be conducted on systems hardware and should include forecasts concerning future technologies.
- ▶ The performance management process should include forecasting capability to enable problems to be corrected before they affect system performance.
- ▶ Analysis should be conducted on system failures and irregularities pertaining to frequency, degree of impact and amount of damage.
- ▶ Controls are to be in place to ensure that workload forecasts are prepared to identify trends and to provide information needed for the capacity plan.
- ▶ IT management should establish a planning process for the review of hardware performance and capacity to ensure that cost-justifiable capacity always exists to process the agreed workloads and to provide the required performance quality and quantity prescribed in service level agreements. The capacity plan should cover multiple scenarios. When identified as availability requirements, management should prevent resources from being unavailable by implementing fault tol-

erance mechanisms, prioritizing tasks and equitable resource allocation mechanisms.

- ▶ Management should ensure the timely acquisition of required capacity, taking into account aspects such as resilience, contingency, workloads and storage plans.
- ▶ Performance monitoring tools could be used at various levels such as Systems – server and hard disk, Network, Application and Enterprise level

Key goal indicators and key performance indicators are to be established for all key IT processes based on assessment of current maturity level and expected maturity level of specified process. Some of the key performance management measures such as budgets, user satisfaction, capacity and growth planning, etc are explained below.

Budgets

Budgets allow for forecasting, monitoring and analyzing financial information. They allow for an adequate allocation of funds, especially in an information systems environment where expenses can be cost-intensive.

User Satisfaction

Because of the difficulties associated with measures of frequency of use, and ease of use, some researchers have attempted to develop instruments that will assess a user's satisfaction with a system. The basic belief that underlies this work is that the user satisfaction is highly correlated with system success and at regular intervals management should measure customer satisfaction regarding the services delivered by the IT function to identify shortfalls in service levels and establish improvement objectives. Some of the key areas for measuring user satisfaction are:

- ▶ Percent of IT investments meeting or exceeding expected benefits, based on return on investment and user satisfaction
- ▶ Reported user satisfaction with the installation and accreditation process (lessons learned)
- ▶ Increased user satisfaction with roll out of new technologies
- ▶ Increased user satisfaction with the effectiveness and efficiency of the help desk

Capacity and growth planning

Capacity and growth planning is very important in an information systems environment. The Information processing facility's needs should be continually reassessed to ensure that the operation is running as effectively as possible and to allow for future needs.

Financial Management Practices

Financial management is a critical element of all business functions. In a cost-intensive computer environment, it is imperative that sound financial management practices are in place.

The User Pay Scheme, a form of charge back, can improve application and monitoring of IS expense and limited resources. The cost of IS services, including staff and computer time as well as other relevant costs, is charged back to the end-users, based on a standard formula or calculation. Charge back provides IS and the user with a tool to measure the effectiveness and efficiency of the service provided by the Information Processing Facility.

Compliance with the Service Level Agreement

Compliance with the service level agreement should be periodically audited. This can be achieved through interviewing and surveying users.

Workload

A system workload is the set of resource demands imposed upon the system by the set of jobs that occur during a given time period. The workload can be characterized as a matrix. The rows in the matrix are the set of jobs that occur for the time period under consideration. The columns in the matrix are the hardware, software and data resources of the system. The elements of the matrix are the amounts of each resource demanded by each job. System performance must be defined in terms of a given workload.

Business Process Reengineering (BPR)

BPR is the process of responding to competitive economic pressures and customer demands to survive in the current business environment. BPR involves transforming of a company from one based on functions such as accounting marketing and manufacturing to one based on processes such as order processing and fulfilling customer expectations. It does mean abandoning long-established procedures and looking afresh at the work required creating a company's product or service and deliver value to the customer. The underlying issue is to re-organize the company according to its few fundamental workflows, which involves breaking down functions and their hierarchy. For example, the concept of a process for airlines would be "Process is not about selling tickets but about moving people to their destinations".

Documentation Standards

Documentation consists of documents and records, which describe the system and procedures for performing a data processing task. It is a means of communicating both the essential elements of the data

processing system and the logic followed by the computer programs. Documentation is a part of any properly implemented data processing system. It is the permanent written record of system functions incorporating the specifications as well as the operations of a system. Maintaining documentation is a continuing function

Management's problem is to determine the level of documentation needed in the information system. Preparing documentation is a time consuming activity. The benefits should outweigh the costs. Documentation should exist for the primary functions within the IS enterprise. These typically include:

- ▶ Computer operations
- ▶ System software
- ▶ Hardware and software acquisition and maintenance.
- ▶ Application software
- ▶ Management reporting
- ▶ Physical and logical reporting
- ▶ Physical and logical security
- ▶ Short and long term planning
- ▶ Time reporting
- ▶ Human resource management

Documentation Standards determine the type and extent of documentation maintained within the enterprise for various types of IT activities and operations. Documentation provides guidance and is useful in ensuring that standard procedures are followed across the enterprise. Further, documentation facilitates monitoring, review and audit of the specific processes and activities. For example in a SDLC process, documentation standards could include the following:

- ▶ Program documentation is communicated to the concerned staff and enforced
- ▶ SDLC methodology ensures that documentation created during information system development or modification projects conforms to these standards
- ▶ Provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programs created as part of every information system development or modification project.
- ▶ Provide standards covering test requirements, verification, documentation, and retention for the testing of the total system as a part of every information system development or modification project.
- ▶ Provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained.

Auditing IT Management

Audit of IT management could be done from different perspectives such as quality, compliance or security. Depending on objective of the audit, detailed control objectives would be prepared as relevant to the business processes of the enterprise and these would be used as benchmark for evaluating the existing IT management practices. The primary objective of IS Audit of IT management practices is to provide management with reasonable assurance that identified IT management practices are implemented as designed to meet business objectives and where there are significant control weaknesses, to substantiate the resulting risks and advise management on corrective actions. A step-by-step approach for auditing IT management includes:

1. Identify Audit Objectives and Scope
2. Choose strategy for using relevant guidelines
3. Identify / Select IT management practices to be audited
4. Select Control Objectives as relevant
5. Extend Control Objectives by adding Business Process / IT controls
6. Identify relevant Risks for identified IT process
7. Identify Management Guidelines/benchmarks
8. Prepare Audit program, procedures and checklist as per above steps
9. Perform the audit and identify the control weaknesses or gaps
10. Prepare draft report discuss the report with auditee
11. Prepare final report
12. Presentation to senior management

Summary

This chapter has provided an overview of Information Systems Management Practices. Practices cover practical aspects of day-to-day functioning of all key activities of an enterprise. Information System practices are an important aspects of any enterprise management as they impact how business goals and objectives are achieved. This chapter has provided an overview of key aspects of Human resource Management, which is one of most important asset of any enterprise. Practices. Some of the critical IS management practices such Performance Management measures; User satisfaction and documentation Standards have been explained in this chapter. Enterprises in the present digital era aspire to be knowledge organizations, which learn and adapt best practices to survive and thrive in this competitive digital era. This requires enterprises to be on the ladder of continuous improvement. Benchmarking is one of the basic tools, which helps enterprises to compare their practices with other competitive entities or recognized international standards. Finally, step-by-step approach to auditing IT Management practices is outlined.

References

- ▶ Chapter 1 of Information Systems control and audit by Mr. Ron Weber, 2002 edition, published by Pearson education (Singapore) Pte. Ltd, Indian Branch, Delhi
- ▶ COBIT Control Objectives (www.isaca.org)



5 IT Change Management

✂ Learning Goals ✂

This chapter deals with Information technology change management. The learning goals of this chapter are:

- ▶ Understand different aspects of IT infrastructure management
- ▶ Methodology of Configuration Management
- ▶ Need for change and change management
- ▶ Key areas and impact of IT Change Management
- ▶ Overview of change Management policies and procedures
- ▶ Need for controls for effective Change Management
- ▶ How to audit change management

Key Objectives

Change has been described as the only permanent thing in this world. The dynamically IT environment and changing nature of business environment demand change to be implemented on a constant basis. Change is imperative for growth. However, change has to be managed and monitored. This chapter deals with key components of IT Change management such as IT infrastructure management, Configuration Management, etc. It also explains the need for change and change management. Key areas and impact of IT Change Management are highlighted and illustrated. Every key aspect of management has to be supported by proper policies and procedures. As change management is critical aspect of IT management, change Management policies and procedures have been explained briefly. Further, it is important that changes are properly controlled. The relevant controls for effective Change Management are explained. Finally, methodology of auditing change management is provided.

IT Infrastructure Management

IT infrastructure encompasses all IT assets used in the enterprise. As enterprises are increasingly dependent on IT for performing business processes and the failure of IT can impact business and its continuance, it is critical to have a good system of IT infrastructure management. COBIT defines classifies IT resources into the following five categories:

1. Data: objects in their widest sense (i.e., external and internal), structured and non-structured, graphics, sound, etc.
2. Application systems are understood to be the sum of manual and programmed procedures.

Module 6, Chapter 5

3. Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.
4. Facilities are all the resources to house and support, information systems.
5. People includes staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

Implementing security makes it imperative to have a comprehensive list of all IT assets and information of enterprise so as to define appropriate access levels as per organization structure.

Configuration Management

IT configuration includes all IT components and IT configuration management refers to the system of identifying and recording all IT assets and their physical location. IT Configuration controls refer to the system of regular verification program which confirms their existence and controls which prevent unauthorized alterations, verify physical existence and provide a basis for sound change management

IT Configuration management to be effective needs to have a system of asset tracking, configuration change management, checking for unauthorized software, software storage controls, software and hardware interrelationships and integration and use of automated tools. Some of the best practices relating to IT configuration management are:

- ▶ Only authorized and identifiable configuration items are recorded upon acquisition.
- ▶ Provide for authorized disposal and consequential sale of configuration items.
- ▶ Keep track of changes to configuration (e.g., new item, status change from development to prototype).
- ▶ Logging and control is an integrated part of configuration recording system including reviews of changed records.
- ▶ Baseline of configuration is standard configuration of items is kept as a checkpoint to return to after changes.
- ▶ Configuration records reflect actual status of all items including history of changes.
- ▶ Existence and consistency of recording of the IT configuration is periodically checked.
- ▶ Clear policies restricting use of personal and unlicensed software is developed and enforced.
- ▶ Use of virus detection and remedy software.
- ▶ Periodical check of organization's personal computers for unauthorized software.
- ▶ Compliance with requirements of software license is reviewed on a periodic basis.

- File storage area (library) is defined for all valid software items in key phases of SDLC.
- File storage area is separated from development; testing & production file storage area.
- Critical components of IT resources are appropriately identified and maintained.
- Current and future processing demands are measured and provide input to the IT resource acquisitions process.
- Software is labeled, inventoried and properly licensed.
- Library management software is used to produce audit trails of program changes and to maintain program version numbers, creation-date information and copies of previous versions.

Need for Change and Change Management

Change is key aspect of any organization. The dynamically IT environment and changing nature of business environment demand change to be implemented on a constant basis. Change is imperative for growth. However, change has to be managed and monitored. Changes could encompass any of IT components such as Facilities, Technology, Applications, Data and People and related policies, procedures and practices are properly controlled. As changes affect business processes, it is critical to implement effective system of change management policies and procedures. The relevant controls and control objectives for effective Change Management are explained later in this chapter.

Key Areas and Impact of IT Change Management

Changes could occur in any of the IT Resources or related controls such as Facilities, Technology, Applications, Data, People and Controls – policies, procedures, practices and organization structure. The key areas, which are impacted by changes, are different components of Information Architecture including information systems and related technology. IT change management could impact the following:

- Configuration management
- Achieving business objectives
- Accounting of all IT components
- Controls which, prevent unauthorized alterations,
- Controls for verifying physical existence
- Change management procedures

Overview of Change Management Policies and Procedures

The IT process “Manage Changes” has to be effectively controlled so as to ensure that the business goal of minimizing the likelihood of disruption, unauthorized alterations and errors. Effective change management requires a management system, which provides for the analysis, imple-

Module 6, Chapter 5

mentation and follow-up of all changes requested and made to the existing IT infrastructure. The Critical Success Factors for effective change management as outlined in COBIT Management guidelines are:

- Change policies are clear and known and they are rigorously and systematically implemented
- Change management is strongly integrated with release management and is an integral part of configuration management
- There is a rapid and efficient planning, approval and initiation process covering identification, categorization, impact assessment and prioritization of changes
- Automated process tools are available to support workflow definition, pro-forma work-plans, approval templates, testing, configuration and distribution
- Expedient and comprehensive acceptance test procedures are applied prior to making the change
- A system for tracking and following individual changes, as well as change process parameters, is in place
- A formal process for hand-over from development to operations is defined
- Changes take the impact on capacity and performance requirements into account
- Complete and up-to-date application and configuration documentation is available
- A process is in place to manage co-ordination between changes, recognizing interdependencies
- An independent process for verification of the success or failure of change is implemented
- There is segregation of duties between development and production

Controls for Effective Change Management

IT process 6 of COBIT domain of Acquisition and Implementation: Manage changes provides control objectives for managing the process of change. These controls can be adapted as required by the enterprise as per nature of business, technology implementation and type of organization structure. The controls relating to changes are given below:

- IT management should ensure that all requests for changes, system maintenance and supplier maintenance are standardized and are subject to formal change management procedures. Changes should be categorized and prioritized and specific procedures should be in place to handle urgent matters. Change requestors should be kept informed about the status of their request.
- A procedure should be in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality.

- ▶ IT management should ensure that change management and software control and distribution are properly integrated with a comprehensive configuration management system. The system used to monitor changes to application systems should be automated to support recording and tracking of changes made to large, complex information systems.
- ▶ IT management should establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational and management assessment prior to implementation. The emergency changes should be recorded and authorized by IT management prior to implementation.
- ▶ The change process should ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.
- ▶ IT management should ensure maintenance personnel have specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorized access to automated systems.
- ▶ IT management should ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc.
- ▶ Specific internal control measures should be established to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.

Auditing IT Change Management

Audit objectives for IT change management could include ensuring that:

- ▶ Only approved changes were made
- ▶ All changes are accounted for
- ▶ Current libraries (source and object) reflect most recent changes
- ▶ Change control procedure variances are recorded and accounted for between:
 - ▶ Purchased and in-house applications
 - ▶ Applications and system software
 - ▶ Vendor treatment of change control

Auditing IT change management requires understanding:

- ▶ Organizational policies and procedures relating to: information systems planning, change control, security and system development life cycle
- ▶ IT policies and procedures relating to: formal SDLC methodology, security standards, testing standards, independent quality assurance, implementation, distribution, maintenance, emergency change, software release and version control of systems.

Module 6, Chapter 5

- ▶ Applications development plan and Change control request form and log
- ▶ Vendor contracts relating to applications development services

This is followed by evaluation of controls relating to:

- ▶ Methodology used for prioritizing system change requests from users
- ▶ Emergency change procedures as provided in operation manuals
- ▶ Formal change control procedure of user and development groups
- ▶ Change control log relating to resolution of changes
- ▶ User satisfaction of turnaround of change requests in terms of timeliness and cost
- ▶ Changes have resulted in program and operations documentation change
- ▶ Changes are made as documented
- ▶ Current documentation reflects changed environment
- ▶ Change process is being monitored for improvements in acknowledgment, response time, response effectiveness and user satisfaction with the process
- ▶ Maintenance to Private Branch Exchange (PBX) system is included in the change control procedures

Summary

Change management process has to be well developed and consistently followed for all changes so as to ensure there are no exceptions. The change management process, to be efficient and effective, requires understanding of the IT infrastructure and related systems. This chapter has provided an overview of the controls required to ensure all changes are subject to thorough planning and impact assessment to minimize the likelihood of post-production problems. Some of the key controls relating to change management include: approval process for changes, documentation management and formal tracking of changes. Finally, audit process for managing changes has been briefly described.

References

- ▶ IT Audit articles on <http://www.itaudit.org>



6 Organization Structure & Controls in IT Department

✂ Learning Goals ✂

This chapter deals with Information Systems Organization Structure and Controls in IT department. The key learning goals are:

- ▶ Distinction between Project Management structure and Line Management structure
- ▶ Defining Roles and responsibilities in an IT department
- ▶ Segregation of duties and related techniques
- ▶ Identifying Incompatible functions
- ▶ Defining access to data
- ▶ Auditing IT organization structure and controls

Key Objectives

This chapter deals with Information System Organization structure in an enterprise with particular relevance to an IT Environment. The objective of this chapter is to provide understanding of structuring of the enterprise to ensure appropriate segregation of duties is achieved and access is provided to information assets as per organization chart. If IT is not outsourced in an enterprise, there could be two types of organization structure: project management structure dealing with management of projects and line management structure dealing with organization structure relating to regular operations. This chapter also deals with segregation of duties in an IT environment and explains the need for ensuring appropriate segregation of duties in an IT environment. Finally, methodology of auditing IT organization structure and controls is provided.

Organizational Structure and IT controls

Management is responsible for affecting the organizational structure and its elements. Organizational control techniques include documentation of:

- ▶ Reporting responsibility and authority of each function
- ▶ Definition of responsibilities and objectives of each function
- ▶ Policies and procedures
- ▶ Job descriptions
- ▶ Segregation of duties

Module 6, Chapter 6

Responsibilities and objectives: Each IT function must be clearly defined and documented, including systems software, application programming and system development, database administration and operations.

Policies and procedures: These are standards and instructions that all IT personnel must follow when completing their assigned duties. Policies establish rules or boundaries of authority delegated to individuals in the enterprise. Procedures establish instructions that individuals must follow to complete their daily assigned tasks. Documented policies should exist in IT for:

- ▶ Use of IT resources
- ▶ Physical security
- ▶ Data security
- ▶ Online security
- ▶ Microcomputer use
- ▶ Reviewing, evaluating and purchasing hardware and software
- ▶ System development methodology
- ▶ Application program changes

Job descriptions: Job descriptions and procedures establish instructions on how to do the job and policies define the authority of the employee. All jobs must have a current, documented job description readily available to the employee.

Segregation of duties: Traditional control technique aimed at separating conflicting job duties, primarily to discourage fraud, because separating duties makes collusion necessary to commit a fraud. This also builds system of internal check where work of one staff is checked automatically by another staff during the course of work. Some examples are:

- ▶ Database administration from data processing
- ▶ Application programming into individual applications
- ▶ Systems analyst from programming

Segregation of duties is done to ensure that no single person has complete control over a transaction through its initiation, authorization, recording, processing and reporting. The objective is to minimize incompatible functions, which are not conducive to good internal control structure. Examples of segregation of duties from perspective of controls should encompass the following:

- ▶ Just minimum access
- ▶ Transaction authorization – maker and checker
- ▶ Exception reporting
- ▶ Custody of assets
- ▶ Access controls
- ▶ Authorization forms
- ▶ User authorization tables
- ▶ Audit trails

- Audit
- Application controls

It may not be always feasible to implement all the required controls. However, lack of controls could be countered by having compensating controls. Compensating controls for lack of segregation of duties encompass the following:

- Audit trails
- Reconciliation
- Exception reporting
- Transaction logs
- Supervisory reviews
- Independent reviews

Management Structure

The organization structure determines effectiveness and efficiency of the general and application controls, segregation of duties, custody of assets and data and management practices in the IS department. If the IT operations or key business processes related to IT are done internally within the enterprise, there could be two types of management:

- Project management: Responsible for implementing IT projects within framework of project management guidelines.
- Line management: Responsible for regular business processes and operations

Project Management Structure

In project management, project requests are submitted to and prioritized by the steering committee. The project manager, who may be a non-IS staff member, should be given complete operational control of the project and be allocated the appropriate resources for the successful completion of the project. Project Management is considered as the art and science of converting vision into reality. Projects are the engines of change. Modern Project Management (MPM) discipline helps in managing change and transition more effectively. Effective project management will require establishing appropriate project management framework defining the scope and boundaries of the project and also defining roles and responsibilities of different persons associated with the project. The key aspects of project management include defining project ownership, clearly outlining user involvement, implementing project management plan and methodology and quality assurance methods and plans. IS auditors may be included in the project team as control advocates and experts. They also provide an independent, objective review to ensure that the level of commitment of the responsible parties is appropriate.

Line Management Structure

Line management Structure

The Information system management subsystems in an enterprise attempt to ensure that the development, implementation, operation and maintenance of information systems proceed in a planned and controlled manner. They function to provide a stable environment in which information systems are built and operated on a day-to-day basis. Several levels of management subsystems have been identified corresponding to the enterprise hierarchy and major functions performed within a data processing installation.

Top management

Top management of the enterprise must ensure that the data processing installation is well managed. It is responsible primarily for long run policies decisions on how computers will be used in the enterprise.

IS Management

IS management has overall responsibility for planning and control of all computer activities. It also provides inputs to top management's long run policy decision making and translates long run policies into short run goals and objectives.

Systems Development Management

Systems Development Management is responsible for the design, implementation and maintenance of application systems.

Programming Management

Programming management is responsible for programming new systems, maintaining old systems and providing general systems support software.

Data administration

Data administration is responsible for the control and use of an enterprise's data including the database and library of application system files.

Security administration

Security administration is responsible for the physical security of the data processing and IS programs.

Operations Management

Operations Management controls the day-to-day operations of data processing systems. It is responsible for data preparation; the data flow through the installation, production running of systems, maintenance of hardware and sometimes maintenance of program and file library facilities.

Quality assurance management

Quality assurance management undertakes an in-depth quality assurance review of data processing in each application system. This review involves a detailed check of the authenticity, accuracy and completeness of input, processing and output.

Defining Roles and Responsibilities in IT department

Roles and Responsibilities

The most critical factor in ensuring Information Systems security is to fix responsibility to the staff as per their specific responsibilities. At the generic level, the organization's work culture should ensure that information Systems security is the responsibility of everyone who can affect the security of an Information Systems system. However, the specific duties and responsibilities of various individuals and organization entities vary considerably based on nature of business, organization structure and organization's policies. Typically, roles and responsibilities in an organization involved with Information Systems security could include the following groups:

- ▶ Senior management,
- ▶ Security/functional managers/application owners,
- ▶ Information Systems security management,
- ▶ Technology providers,
- ▶ Supporting enterprises, and
- ▶ Users.

Enterprises, like individuals, have unique characteristics, and no single template can apply to all. Smaller enterprises, in particular, are not likely to have separate individuals performing many of the functions described here. Even at some larger enterprises, some of the duties described here may not be staffed with full-time personnel. What is important is that these functions be handled in a manner appropriate for the enterprise. Senior management has ultimate responsibility for the security of an enterprise's Information Systems.

Duties and Responsibilities

In any enterprise, the specific duties and responsibilities would be dependent on the policies, technology and nature of business. A brief explanation of illustrative list of duties and responsibilities in IT department are given below.

Data entry

The data entry supervisor is responsible for ensuring whether the data is authorized, accurate and complete when entered into the system. Components in the input subsystem are responsible for bringing information into a system. The information takes two forms: first, it may be raw data to be processed and perhaps applied against the database; sec-

ond, it may be instructions to direct the system to execute particular processes, update or interrogate particular data, or prepare particular types of output. Both types of information input must be validated. Any errors detected must be controlled so that the input resubmission is authentic, accurate, complete, unique and timely.

File Librarian

The file librarian is responsible for recording, issuing, receiving and safeguarding all programs and data files that are maintained on computer tapes or disks in an Information Processing Facility. Managing the enterprise's library of machine-readable files involves three functions.

1. Files must be used only for the purposes intended. Control must be exercised over program files, data files and procedure files.
2. Storage media used for files must be maintained in correct working order.
3. File backup strategy and file retention strategy must be implemented.

Within the IT department, responsibility for managing files is vested in a file library section. It is a substantial management problem to ensure correct control and use of these files. A basic prerequisite for effective and efficient management is an orderly filing system. The filing system must encompass procedures for storing and retrieving the files, storage media and maintaining records of events that occur to the files and storage media.

Operations management team

Operations management is responsible for the daily running of hardware and software facilities so that the production application system can accomplish their work and development staff can design implement and maintain systems. Though there are some variations across the enterprises, the operations group within the IT department undertakes seven major functions:

- ▶ Computer operations
- ▶ Communication network control
- ▶ Data preparation
- ▶ File library
- ▶ Documentation library
- ▶ Performance monitoring

In some ways, the functions of operations management appear routine and mundane. If they are not carried out properly, however, some serious consequences can occur. For example, well-designed program controls can be compromised if an operator uses a console terminal to alter the state of the computer internal memory; well-designed program code

will execute inefficiently if there is an undesirable job mix in the machine.

Security Administration

The security administrator in a data processing enterprise is responsible for matters of physical security. In other words, the security administrator attempts to ensure that the physical facilities in which the systems are developed, implemented, maintained and operated are safe from threats that affect the continuity of operation. In small enterprises that use turnkey systems- that is, hardware and software that have been purchased as a package rather than developed in house – there may be no data processing staff and as a consequence, no one to assume the role of security administrator. If an enterprise has its own data processing staff but insufficient work exists to justify an ongoing, separate security administrator position, responsibility for security matters may be vested in the operations manager. Since the operation manager is responsible for the day-to-day running of hardware and software systems, physical control over these facilities seems a natural extension of these responsibilities.

In large enterprises, there may be sufficient work to justify a separate security administration position. In some cases, the security administrator may report directly to the data processing manager or to the executive in charge of information systems in the enterprise. In other cases, computer security administrator may report to an executive who assumes overall responsibility for all security matters with the enterprise.

Segregation of Duties and Related techniques

Segregation of duties is a traditional, non-computer control technique aimed at separating conflicting job duties, primarily to discourage fraud, because separating duties makes collusion necessary to commit a fraud. Such separation can also force an accuracy check of one-person work by another, so that employees to some extent police each other.

Organizations have their lines of reporting, defined roles and responsibilities and established controls. Given this structure, the IS Auditor should examine the organization of the IT department to ensure that adequate division of duties exists, that recruitment and staff relations procedures are conducive to control, and that training is adequate. One of the more important aspects of organization and management is the concept of division of duties. This is a sound principle of internal control and should be applied to the computing area. The role definitions should be such that responsibility for all aspects of processing data does not rest with a single individual or department. The functions of initiating, authorising, inputting, processing and checking of data should be separated. This ensures that no one person has complete control over a

particular function; therefore, abuse of that function (fraud, etc.) is not possible without collusion between two or more individuals.

Key concepts of segregation in Computerized Information Systems

Although the principles of audit do not undergo any change under IS audit or under computerized set-up the IS auditor should consider the key components of IS environment including organization structure as they affect the design of accounting system and related controls. In an IS center since the work is of specialized nature the number of persons involved may be less and in some cases only one person may be involved in such work. This indicates the vulnerability of automation resulting in total stoppage in case of sudden non-availability of staff at times of crisis. Hence, it is necessary to have stand-by staff to take care of such eventualities. Duties of system programmer/designer should be segregated from person operating the system and there should be separate persons to perform the above two functions. The Systems person will only do modifications/improvements to programs and the operating person will only use such programs without having the right to do any modifications.

Factors to Consider in Segregation of Duties in Computerized Information Systems

Information Security Office is the corporate-level computer security policy-making organization responsible for the creation, evaluation, and administration of computer security policy, guidelines, and procedures in support of the organization security program. All applications defined by executive sponsors (or users' managers for local systems) as critical to their operations must be supported by an up-to-date, tested contingency plan. The critical factors to be considered in segregation of duties in a computerized information system are:

- ▶ Nature of Business operations
- ▶ Managerial policy
- ▶ Organization structure with job description
- ▶ Information technology resources deployed such as:
 - ▼ Operating System
 - ▼ Networking
 - ▼ Database
 - ▼ Application Software
 - ▼ Technical staff available
- ▶ IT Services provided in-house or out-sourced
- ▶ Centralized or decentralized IT operations

Based on the above factors, appropriate segregation of duties has to be achieved. The most important aspect is to define access to information based on "need to know" or "need to do" basis. It is important to define

the information architecture of the enterprise. Based on which the data dictionary is to be defined. Access to each class / type of data has to be defined based on the specific job responsibility. The over-riding principle is access to information is restricted unless specifically permitted. Further, access has to be restricted considering the type of processing, which can be done. For example, a user clerk in warehouse can only enter data pertaining to Goods Received Note (GRNs) whereas his supervisor can only approve. Attached is an access matrix of an ERP Package, which shows how access has been restricted to each of the options (run, add, delete, update) for each of the specific functions.

Segregation of Duties

IT process 4 of COBIT control objectives titled determine IT organization and relationships highlights the importance of segregation of duties. It states that Management should ensure that all personnel in the organization have and know their roles and responsibilities in relation to information systems. All personnel should have sufficient authority to exercise the role and responsibility assigned to them. Roles should be designed with consideration to appropriate segregation of duties. No one individual should control all key aspects of a transaction or event. Everyone should be made aware that they have some degree of responsibility for internal control and security. Consequently, regular campaigns should be organized and undertaken to increase awareness and discipline.

Management should formally assign the responsibility for assuring both the logical and physical security of the enterprise's information assets to an information security manager, reporting to the enterprise's senior management. At a minimum, security management responsibility should be established at the enterprise-wide level to deal with overall security issues in an enterprise. If needed, additional security management responsibilities should be assigned at a system specific level to cope with the related security issues.

Senior management should implement a division of roles and responsibilities which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs and positions. In particular, a segregation of duties should be maintained between the following functions:

- ▶ Information systems use
- ▶ Data entry
- ▶ Computer operation
- ▶ Network management
- ▶ System administration
- ▶ Systems development and maintenance

Module 6, Chapter 6

- Change management
- Security administration
- Security audit

Identifying Incompatible Functions

Access to information in information systems is based on job description. Segregation of duties has to be as per the organization structure and to meet the needs of the business. However, in general, there are some specific functions which when combined could increase the risk. Some examples of such combination of incompatible functions in IT are:

- Systems software programming group and application programming group
- Database administration group and other data processing activities
- Computer hardware operations and other groups
- Physical, data, and online security group(s) and other IS functions

Information Access Classification

Based on the Confidentiality, Integrity and Availability classification done for the IT systems, each of the IT systems will have appropriate access classification. Most business organizations follow a four level classification for providing access to the information systems:

- **Unclassified:** Considered publicly accessible. There are no requirements for access control or confidentiality.
- **Shared:** Resources that are shared within groups or with people outside of your organization.
- **Company Only:** Access to be restricted to your internal employees only.
- **Confidential:** Access to be restricted to a specific list of people.

Controlling access to various information assets is thus based on defining who has access to what information through Access Control Lists (ACL). The ACLs are implemented through various security measures like data base access control tables as well as perimeter security devices like access control cards and firewalls. Final responsibility for defining the information classification and access permissions rests with the owner of the information assets. For example: specific portions of HR database would be identified and classified for the defined level of access. Only the HR database owner, i.e. the Head of HR, should be responsible for this classification.

Job descriptions

These communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee. All jobs must have a current, documented job description readily available to the employee.

Job descriptions establish responsibility and the accountability of the employee's actions

Segregation of Duties for Database Administration

As data is stored in a common database, which is centrally available, and easily accessible to all users, it is important to ensure restricted access to this data based on the specific responsibility assigned to each of the staff. Thus, segregation of duties in a database could be done in the following manner:

Access to the Database

User access to the database can be restricted through the use of passwords. These restrictions apply to individuals, terminal devices and programs. For passwords to be effective adequate procedures are required for changing passwords, maintaining secrecy of passwords and reviewing and investigating attempted security violations. Relating passwords to defined terminal devices, programs and data helps to ensure that only authorized users and programs can access, amend or delete data. For example, the credit manager may give salesmen authority to refer to a customer's credit limit, whereas a warehouse clerk may not have such authorization. User access to the various elements of the database may be further controlled through the use of authorization tables. Improper implementation of access procedures can result in unauthorized access to the data in the database.

Segregation of Duties

Responsibilities for performing the various activities required to design, implement and operate a database are divided among technical, design, administrative and user personnel. Their duties include system design, database design, administration and operation. Maintaining adequate segregation of these duties is necessary to ensure the completeness, integrity and accuracy of the database. For example, those persons responsible for modifying personnel database programs should not be the same persons who are authorized to change individual pay rates in the database.

Database Controls

There are new job designations and responsibilities in a computerized information system. For example, in a database environment, it is very critical to define the job responsibility of the Database administrator. The organization must have a data base administrator (DBA) who must be responsible for the definition, enterprise, protection, and efficiency and content of the database.

DBA responsibilities

- Set up new installation, perform upgrades and migrations
- Perform corrective steps and trouble shooting
- Advise information systems management in the selection of hardware and software
- Plan the structure of the data base
- Document the data base controls
- Consult with users on data enterprise and retrieval methods.
- Establish security procedures and procedures for recovery in the event of data base destruction.
- Monitor the usage of the data base design.
- All major modifications (both in house and otherwise) must be approved by the DBA.
- The DBA must work with the user in finalizing the data base design
- The data base management systems (DBMS) must have procedures to restrict unauthorized access to data.
- The DBA or a responsible person must adequately control the DBMS library.
- There must be adequate controls to prevent access to the database when it is not under the control of the DBMS.
- The DBA or a responsible person must review periodically the DBMS library to ensure that no unauthorized changes have been made.
- The DBA or another responsible person must review the DBMS log.
- All changes to the DBMS library must be approved and logged by the DBA or a responsible person
- Conduct performance tuning
- Backup and performance recovery
- Write code, triggers, stored procedures when necessary
- Ensure availability of key mission critical databases
- Load / unload data and perform data synchronisation
- Space and account management
- Manage licences and capacity planning

DA responsibilities

- Undertake strategic data planning, determining user needs; specifying conceptual and external schemes (user-oriented) definitions
- Advising users on data-collection procedures; specifying validation and editing criteria
- Specifying new conceptual and external schema definitions; advising users on how to confirm with new definition
- Specifying retirement policies for data
- Determining end-user requirements or database tools; testing and evaluating end-user database tools

- ▶ Answering end-user queries educating end-users establishing and promulgating high-level policy information; providing conceptual schema and external schema information
- ▶ Developing and promulgating organization wide standards; assisting end users to formulate application controls
- ▶ Monitoring end-user patterns of database user

Separation of Duties between the Information Processing Facility and other Organization Units

In a manual system, separate individuals should be responsible for initiating transactions and custody of assets. As a basic control, separation of duties prevents error from taking place or detects errors and irregularities faster. In a computer system, however, the traditional notion of separation of duties does not always apply. For example, a program may reconcile a vendor invoice against a receiving document and print a check for the amount owed to the creditor. Thus, the program is performing functions that in manual systems would be considered incompatible. Nevertheless, it may be inefficient and, from a control viewpoint, useless to place these functions in separate programs. Instead, separation of duties must be in a different form. Once it has been determined that the program executes correctly, the capability to run the program in production mode and the capability to change the program must be separated.

Controls over Access to Data

In a computer system many different types of controls are used to enhance computer reliability. Some of the major classes of controls that an auditor must evaluate are:

Authenticity controls

Authenticity controls attempt to verify the identity of the individual or process wanting to undertake some action in a system. Examples: passwords, personal identification numbers, digital signatures.

Accuracy controls

Accuracy controls attempt to ensure the correctness of data and processes in a system. Examples: program validation checks that a numeric field contains only numeric; overflow check, financial control total, and hash total.

Completeness controls

Completeness controls attempt to ensure that no data is missing and that all processing is carried through to its proper conclusion. Examples: program validation checks to verify a field is not blank, record sequence numbers, financial control total.

Redundancy controls

Redundancy controls attempt to ensure that a data item is processed only once. Examples: batch cancellation stamps, record sequence numbers, circulating error files, financial control total.

Privacy controls

Privacy controls attempt to ensure that data is protected from inadvertent or unauthorized disclosure. Examples: encryption, passwords, data compaction, inference controls.

Audit trail controls

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

Existence controls

Existence controls attempt to ensure the ongoing availability of all system resources. Examples: database dumps and logs for recovery purposes, duplicate hardware, preventive maintenance, checkpoint and restart controls.

Asset safeguarding controls

Asset safeguarding controls attempt to ensure that all resources within a system are protected from destruction or corruption. Examples: fire extinguishers, physical barriers, passwords, file libraries.

Effectiveness controls

Effectiveness controls attempt to ensure that systems achieve their goals. Examples: regular monitoring of user satisfaction, post-audits, monitoring of frequency of use, periodic cost-benefit analyses.

Efficiency controls

Efficiency controls attempt to ensure that a system uses minimum resources to achieve its goals.

Examples: logs of resource consumption, performance monitoring using hardware and software monitors, regular interviews with system users.

Auditing IT Organization Structure and Controls

Audit objectives could include identifying:

- ▶ Weaknesses in the IT function and its activities caused by ineffective oversight by the IT planning/steering committee

- Organizational structure gaps, overlaps, etc., resulting in the ineffectiveness or inefficiencies in the IT function
- Inappropriate organizational structures, missing functions, insufficient staffing, competency deficiencies, improper roles and responsibilities, data and system ownership confusion, supervisory problems, lack of segregation of duties, etc.
- Systems being developed, modified or implemented that do not meet quality assurance requirements
- Systems being developed, modified or implemented that do not meet security (either logical or physical, or both) requirements
- Contracts, which do not meet the organization's contracting requirements
- Ineffective coordination and communication between the IT function and various other interests inside and outside of the IT function

Documents to be reviewed could include:

- Senior management planning/steering roles and responsibilities
- Organization objectives and long- and short-range plans
- IT objectives and long- and short-range plans
- Organization chart showing the IT function in relation to other functions
- Policies and procedures relating to the IT organization and relationships
- Policies and procedures relating to quality assurance
- Policies and procedures used to determine the IT staffing requirements
- IT function organization chart
- IT function roles and responsibilities
- IT function key position (job) descriptions
- Status reports and minutes of planning/steering committee meetings

The following controls need to be audited:

- The IT planning/steering committee oversees the IT function and its activities and resolves action items
- Appropriateness of the reporting hierarchy for the IT function
- Effectiveness of IT function's location in the organization with respect to providing a partnership relationship with top management
- Senior IT management understand what processes are used to monitor, measure and report on IT function performance
- Key indicators are used to assess performance
- Process for analyzing actual results against target levels to determine the corrective actions taken when actual results do not meet target levels

Module 6, Chapter 6

- Actions taken by management for any significant variances from expected levels of performance
- Users/owners management assess the IT function's responsiveness and ability to provide information technology solutions which meet user/owner needs
- IT management is aware of its roles and responsibilities
- Quality assurance involvement in testing and sign-off on IT project plans
- Security personnel review core operating system and application systems
- Adequacy of security function reports or documentation evaluating information security (both logical and physical) in place or under development
- There is sufficient awareness and consistent application of information security policies and procedures
- Personnel attend information security and internal control training
- Data and system ownership is defined for all information assets
- Data and system owners approved changes made to data and systems
- All data and systems have an owner or custodian who is responsible for the level of control over the data and systems
- Access to all data and system assets is approved by the asset's owner(s)
- Direct line of authority and supervision associated with a position (job) is commensurate with the responsibilities of the incumbent
- Position (job) descriptions clearly delineate both authority and responsibility
- Position (job) descriptions clearly describe the required business, relational and technical competencies
- Position (job) descriptions have been communicated accurately and are understood by the individual
- Position (job) descriptions for the IT function contain key performance indicators which have been communicated to the personnel
- IT staff duties and responsibilities correspond to both the published position (job) descriptions and the organization chart
- Position (job) descriptions are in place for key positions and include organization mandates in relation to information systems, internal control and security
- Accuracy of position (job) descriptions compared to the current responsibilities of the incumbents in these positions
- Nature and extent of compliance with the intended segregation of duties and limitation of functions within the IT function
- IT staffing maintains competence

- ▶ Appropriateness of the position (job) descriptions as a basis for adequacy and clarity of responsibilities and authority and performance criteria
- ▶ Contract administration responsibilities are assigned to appropriate personnel
- ▶ Terms of the contracts are consistent with normal organization standards for contracts and standard contractual terms and conditions have been reviewed and evaluated by legal counsel and their concurrence obtained
- ▶ Contracts contain appropriate clauses with respect to adherence to: corporate security and internal control policies, and standards for information technology
- ▶ Processes and/or structures provide for effective and efficient coordination necessary for successful relationships

Summary

Senior management has to ensure that they set up appropriate type of organization structure depending on the nature of business, type of technology deployment and business objectives so as to ensure that business goals are achieved. Segregation of duties plays a very crucial role in establishing appropriate system of controls. This chapter has outlined the need for organizational controls and the two types of management structures: project management and line management. This chapter has also highlighted the importance of Policy statements and communications from senior management to ensure the independence and authority of the IT function. Management has to ensure that membership and functions of the IT planning/steering committee have been defined and responsibilities identified. The need for Segregation of duties between the different pairs of units such as the following have to be clearly documented, designed, implemented and monitored:

- ▶ Systems development and maintenance
- ▶ Systems development and operations
- ▶ Systems development/maintenance and information security
- ▶ Operations and data control
- ▶ Operations and users
- ▶ Operations and information security

This chapter has also explained briefly the type of controls, which, can be, implemented in various type of line management functions and finally, setting audit objectives and type of audit tests to be performed have been provided.



References

- ▶ Chapter 6 of Information Systems control and audit by Mr. Ron Weber, 2002 edition, published by Pearson education (Singapore) Pte. Ltd, Indian Branch, Delhi.
- ▶ COBIT Control objectives [<http://www.isaca.org>]
- ▶ COBIT management Guidelines [<http://www.isaca.org>]
- ▶ ISACA's IS Audit Guidelines [<http://www.isaca.org>]
- ▶ IFAC's IT Guidelines [<http://www.isaca.org>]

Questions

1. Which of the following is the most critical consideration in providing access to information in an enterprise?
 - A. Job descriptions
 - B. Technical skills
 - C. Work Experience
 - D. Security policy
2. For IT steering committee to be effective, it's members must necessarily include:
 - A. Users
 - B. IT head
 - C. Director
 - D. Functional Heads
3. Which of the following is not a function of the IT steering committee?
 - A. Establish size and scope of IT function
 - B. Set priorities for the IT projects
 - C. Formulate IT procedures and practices
 - D. Review and approve standards, policies and procedures
4. Which of the following is the basis for providing authorization and access to employees in an enterprise?
 - A. Organization Structure
 - B. Nature of Business process
 - C. Type of technology
 - D. Style of management
5. The most critical consideration in IT strategy planning from perspective of IT governance is:
 - A. Senior management should develop and implement long- and short-range plans
 - B. IT issues as well as opportunities are adequately assessed and reflected
 - C. IT is aligned with the mission and business strategies of the

- enterprise.
- D. Strategic plan must address and help determine priorities to meet business needs
6. The primary objective of segregation of duties is:
- A. Distribution of work responsibilities as per experience
 - B. Prevention/Monitoring of accidental or purposeful errors/omissions
 - C. Distribution of work as per technical skills
 - D. Provide better service to customers
7. Which of the following statement relating to policies is incorrect?
- A. Provide management guidance and direction overall effective deployment of Information and its activities.
 - B. Provide details of actions to be taken for preventing, detecting, correcting and reporting security lapses.
 - C. Refers to specific security rules for particular systems.
 - D. State the high-level enterprise position and scope.
8. Which of the following statement relating to practices is correct?
- A. Refer to implementation aspects for various Information systems and related activities
 - B. Outline set of steps to be performed to ensure that a policy guideline is met
 - C. Provide management guidance and direction overall effective deployment of Information and its activities
 - D. Formulated by senior management and represents strategic philosophy
9. Which of the following is most critical for effective implementation of security
- A. Defining and communicating individual roles, responsibilities, and authority
 - B. Having regular external audit of security implementation
 - C. User training covering all aspects of security
 - D. Senior management is well versed with technical aspects of security
10. The most important resource for successful deployment of Information technology in an enterprise is:
- A. Effective Business processes
 - B. Trained Human Resources
 - C. Well-defined Organization structure
 - D. Implementing Latest technology
11. Which among the following combination of roles results has maximum risk
- A. Data entry and Operations

Module 6, Questions

- B. Librarian and Help Desk
 - C. Systems Analysis and Quality Assurance
 - D. Database Administration and Data entry
12. During the preliminary stage of a review of an IT strategic plan, the MOST critical audit procedure is to verify the existence of:
- A. Documented long-range plan for facilities, hardware and system and application software.
 - B. Short-range plans, which has been prepared outlining specific projects.
 - C. Specific assignments for each IT manager that supports completion of short-range plans.
 - D. Methodology for progress reporting and monitoring relating to adequacy of long/short-range plans
13. Security policy to be MOST effective has to be defined, based on:
- A. Technology deployed
 - B. Risk analysis
 - C. User requirements
 - D. Security standards
14. The two overall primary goals of IT Governance are:
- A. Consider critical success factors that leverage IT resources and measure them
 - B. Ensure delivery of information to business and measure using Key Goal Indicators
 - C. Create and maintain system of process/control excellence and monitor business value delivery of IT
 - D. Add value to business and balance risk versus return
15. The primary purpose in management implementing IT controls and IS auditor reviewing these controls is to:
- A. Maintain Data integrity
 - B. Safeguard computers are
 - C. Provide assurance that business objectives are achieved
 - D. Provide proper segregation of duties
16. The MOST critical consideration for an IS Auditor in reviewing access authorizations is to understand the:
- A. IT Resources
 - B. Organization structure
 - C. Functionalities
 - D. Nature of business
17. In reviewing segregation of duties, the IS Auditor as a measure of BEST control would review whether the Security Administrator (SA) is:
- A. Performing functions as defined

- B. Well trained in business processes
 - C. Technically competent
 - D. Aware of the security policy
18. Which of the following is the MOST critical consideration in segregation of duties?
- A. The possibility for a single individual to subvert a critical process is prevented
 - B. Senior management ensures implementation of division of roles and responsibilities.
 - C. Staff is performing only those duties stipulated for their respective jobs and positions.
 - D. Experienced staff review all critical functions performed by junior staff.
19. In an organization providing services of outsourcing, the PRIMARY objective of a Business Continuity Plan (BCP) is to ensure:
- A. Safeguard assets from a disaster
 - B. Redundancy of IT resources
 - C. Continuity of critical business processes as per SLA
 - D. Identify single points of failure relating to Technology.
20. At the preliminary review stage of IT strategic plan; the most critical audit procedure involves verification of:
- A. Short-range plan, which has been prepared outlining the specific project.
 - B. Specific task activities delegated to section manager that support completion of short-range plan.
 - C. Methodology for progress reporting and monitoring relating to adequacy of long range and short-range plan
 - D. Documented long-range plan for facilities, hardware, system software and application software.
21. In addition to defining the policy objective, which of the following is MOST critical to ensure implementation of policy?
- A. Provide adequate allocation of resources
 - B. Establish clear-cut responsibilities.
 - C. Commitment from senior management
 - D. Monitor changes required on a regular basis.
22. The GREATEST risk on account of inadequate IT policies and standards is:
- A. Lack of benchmarks for evaluating the operations
 - B. Security and controls may be compromised.
 - C. Audit opinion on quality of control and security will be open to question.
 - D. Time required for audit is higher.

Module 6, Questions

23. In review of Job description, IS Auditor's concern from control perspective is:
- A. Are current, documented and readily available to the employee.
 - B. Establish instructions on how to do the job and policies define authority of staff.
 - C. Establish responsibility and the accountability of the employee's actions.
 - D. Communicate management's specific expectations for job performance
24. The MOST critical consideration for an IS Auditor in reviewing access authorizations is to understand the:
- A. Security policy
 - B. IT Resources
 - C. Functionalities
 - D. Organization structure
25. The MOST critical consideration in preparing a security policy is the:
- A. Analysis of the assets.
 - B. Analysis of the perceived risks.
 - C. Review of intellectual property to be safeguarded.
 - D. Availability of tools to monitor security.
26. Which of the following additional duties performed by the information security manager poses the GREATEST risk to the organization?
- A. Maintaining custody of documents
 - B. Operating computer hardware
 - C. Entering data for processing
 - D. Programming
27. Which of the following is MOST likely to be result of inadequate IT policies and standards?
- A. Absence of guidelines and benchmark
 - B. Security and controls may be compromised
 - C. Audit opinion on quality of control and security will be open to question.
 - D. Time required for audit is higher.
28. The MOST critical factor to be considered in segregation of duties in an IT environment is:
- A. Business operations
 - B. Security policy
 - C. Organization structure
 - D. IT resources

Module 6, Questions

29. In auditing outsourcing, which of the following is the IS Auditor most likely to consider for formulating the audit scope and objectives:
- A. Benefits of outsourcing
 - B. Technical skills of service provider
 - C. Service level agreement
 - D. Quality of services provided
30. The primary objectives for auditing IT change management is to ensure that:
- A. Only approved changes were made
 - B. All changes are documented
 - C. Change control procedure variances are recorded and accounted.
 - D. Latest version of software is used

Answers

QUESTION No	1	2	3	4	5	6	7	8	9	10
ANSWERS	A	B	C	A	C	B	C	A	A	B

QUESTION No	11	12	13	14	15	16	17	18	19	20
ANSWERS	D	A	B	D	C	B	A	A	C	D

QUESTION No	21	22	23	24	25	26	27	28	29	30
ANSWERS	B	A	C	D	B	C	B	C	C	A



Module 7:

IS Audit Process

1 Information Systems Risks and Controls

✂ Learning Goals ✂

- ▶ Understand the fundamental requirements of Information Security
- ▶ Understand IS risk and its elements
- ▶ Gain knowledge on IS risk assessment and its difference from IS risk management
- ▶ Gain knowledge of use of use of IS risk assessment as key to planning and performing an audit
- ▶ Gain knowledge of an integrated approach to Information Security strategy
- ▶ Gain understanding of IT Governance and it elements

Information Systems Auditing Fundamentals

Ron Weber in his book “Information Systems Control and Audit” defines, Information Systems Auditing as the process of collecting and evaluating evidence to determine whether a computer system:

- ▶ safeguards assets
- ▶ maintains data integrity
- ▶ allows organizational goals to be achieved effectively and
- ▶ consumes organizational resources efficiently

Conventional auditing such as financial and operational audits involves an independent and competent professional who objectively obtains and evaluates evidence to either a) evaluate the management’s assertions as regards the economic entity or the audit subject or b) opine with regard to the stated audit objectives. The auditor is required to conduct such audit in conformance with the standards of auditing.

Both conventional and Information Systems Auditing follow broadly the same process as regards the auditing process. However in Information Systems auditing the basic premise of audit is to independent conduct an appraisal of the Risk Management as regards the risks to business arising from the IT and related risks.

The broad phases in an IS audit would include:

- ▶ Preliminary Review
- ▶ Audit Planning
- ▶ Conduct of Audit Procedures – Compliance and Substantive Audit procedures

Module 7, Chapter 1

- ▶ Discussion and agreement on findings and recommendations
- ▶ Reporting and Follow Up

Hence the fundamental principles of audit do not change; however, the perspective of audit and the methods, tools and techniques to achieve the audit objectives do undergo a change. In an Information Systems Audit the focus is on the risks arising from the use of technology for information processing and related business processes. Hence this requires the audit professional to have knowledge and expertise to evaluate the Information Systems Risks and Controls and its impact on the related business processes.

IS Auditors have to assess existing risks, security and controls and may be required to assure management that the risk management strategy is adequate and appropriate. Hence it is pertinent that the IS Auditor be aware of the nature of IS risks, threats, vulnerabilities and types of security and controls available. Further, auditors should be in a position to evaluate the risk management measures and to identify the residual risks.

Information and Information Systems controls in an IT driven environment suffer from significant inherent risks such as data loss, corruption of data, risk of unauthorised access to and modification to data in electronic form, risk of logical access to instruction sets, datafiles and critical systems settings etc. The environment also enables vast amounts of information to be stored on relatively small electronic media; however, despite the small size, the results of loss of such data and loss of integrity can be significant.

Besides, computer systems are highly vulnerable to error, omission and abuse, both from inside and outside the data processing networks. The rapid progress in technology and knowledge and accessibility to users of techniques of exploiting the information in electronic environment presents ever increasing risks. Computer crime presents itself as a significant risk to the organizations, with the capability of access and tampering of information by cyber criminals who have cross-border access to such information. Hence in such situations, tracing the identity of the criminals and booking them under the law presents with significant problems.

Most computer failures are however due to errors, negligence and low-tech manipulations by insiders. The solutions are usually straight forward but seldom implemented effectively due to the technological complexity and more due to improper control structures. IS Auditors are required to provide reasonable assurance to management that computer data and related controls are protected and data is protected against the risks inherent to such environments.

Some of the risks specific to Information Technology environments are given below:

- ▶ The data handling capacity of the computer combined with telecommunication technology allows users to access and manipulate large quantities of data with ease and irrespective of the physical location. This significantly increases the potential risk of exposure or damage to business.
- ▶ Computerised Information Systems are highly distributed, hence a single transaction cycle (e.g. e-banking) may span several systems and processes across several locations connected using dedicated or, more commonly, public telecommunication lines. This raises the risks of crimes by abuse and misuse of computer systems to cause unauthorized access and manipulation of data in transit.
- ▶ Online processing of data and validation checks often helps prospective perpetrators to crack/hack passwords and circumvent computer controls
- ▶ Poor controls (such as improper systems settings or more commonly lack of user and management discipline) render the computer resources vulnerable to abuse and attacks.
- ▶ Poor focus on technology risks and related controls and their potential impact causes exposures

Information Security – Fundamental Expectations

Information is one of the critical resources that supports the mission of an organisation and enables achieving the business objectives of the organisation. Every organisation uses and generates a wide range of information that could range from strategic business information, to information relating to day-to-day operations. With the increasing use of technology for achieving information processing, it is not only the information but also the technology that enables the processing of information that has assumed significant importance.

The basic objective of information security requires protecting the fundamental requirements of the organisation's information resources, and comprises:

- ▶ Confidentiality
- ▶ Integrity
- ▶ Availability

Confidentiality

Confidentiality involves the protection of the organisation's sensitive information from disclosure to unauthorized persons and processes or to authorized persons and processes for unauthorized purposes.

Module 7, Chapter 1

Confidentiality threats in an IT environment include intentional as well as unintentional access to sensitive information. A few examples of exposures are given hereunder:

- ▶ Improper application controls in application software may lead to sensitive information being accessed by employees not having need to access such information e.g. a payroll clerk may get accidental access to confidential records of management employees.
- ▶ Hackers and masqueraders could bypass the access controls using either special tools or simply social engineering techniques to get access to sensitive passwords of privileged logins, thereby compromising sensitive business information intended for access only to privileged users. Hackers may even intercept packets in transit over the Internet or unprotected telephone lines to gain unauthorized access to content of e-mail or any other application-to-application data transfers.
- ▶ Masqueraders using trojan codes, may pose as authorized users and get access to sensitive passwords, such as systems administrator passwords or passwords of management users, to get unauthorized access to files containing confidential information. In the recent past there have been a spate of such mails that request Internet banking customers to renew their account information, thus tricking them to disclose their sensitive information such as Internet Banking passwords, PIN etc.
- ▶ Accidental access to spool files used by printers may compromise sensitive information which may otherwise be protected by stringent access controls.

Integrity

Business decisions are based on information on performance, information from external sources, information collated from accounting and other systems etc. Such information may be used for decision making or used for critical submissions to regulatory authorities. Integrity requires that such critical information does not suffer any unauthorized modification, which may result in serious consequences to the business. Integrity also requires that the data that enters the computer systems is complete, since incomplete data suffer risks of improper processing, loss of integrity due to errors etc., Transactions that enter the computer systems should be valid, since computers, unless supported by adequate controls, are not capable of differentiating between valid and invalid transactions. The data entered into, and contained in, the computer should be accurate relative to the need of the computer systems. Integrity also requires that the access to the computer resources granted to users is justified based on their need to know and need to do and that users are provided with the required access to effectively and efficiently conduct their business affairs.

Integrity requires that critical information and related systems processes be protected from either intentional or accidental unauthorized changes. Integrity violations may be caused either by users or outsiders causing intentional modification to the state of information. Integrity violations in an IT environment are also common due to system errors which include corruption of files, power failures leading to unauthorized alteration in the values being transmitted or stored, erroneous program codes leading to alteration of values in datafiles etc; hence the need to prevent the processes from performing any integrity violations.

A few examples of exposures are given hereunder:

- ▶ A Sales executive using data diddling techniques can change the value of travel advance drawn by him.
- ▶ A bank employee not having authority to credit files may tamper with the sanctioned amount of credit facilities by bypassing the application controls and making direct changes to data files or by gaining unauthorized access to the manager's login.
- ▶ Integrity violations in mission critical systems could cause irreparable damage to the business, threats to national security or loss of lives e.g. corruption of tariff data files of Indian Railways, changes in values or parameter files of missile control systems, metrological warning systems, corruption of program codes of autopilot systems used in flight control etc.
- ▶ A common mail user on a webmail portal may gain accidental access to critical systems settings and parameter settings leading to the risks of compromising the mail system security permanently.

Availability

Availability relates to whether the information and information technology processes are available to the business users when required. This requires that the inherent risks of information technology do not pose an obstacle to business and business users.

Availability therefore requires safeguarding the information technology, systems and processes that are essential for supporting information technology processes and related business processes, so as to assure business and business users that the computer systems and related processes critical for conduct of business will be available to authorized users as and when required.

A few examples of exposures are given hereunder:

- ▶ Failure or Improper functioning of power systems that power the computer systems can lead to the computer systems being dysfunctional and hence not available for service e.g. during banking hours, a total power failure, in the absence of necessary backup controls, can result in the suspension of a bank's operations in a Core banking environment

Module 7, Chapter 1

- ▶ Problems with the telephone lines due to flooding, cable faults etc. can result in the last mile problems leading to computer systems being not in a position to establish connection with the parent servers, thereby disrupting business operations e.g. an ATM of a bank may not be available for service if the telecommunications systems experience failure thus causing disruption of service to the customers.
- ▶ Corruption of data residing in computer memory, hard drives and other media can cause loss of transactions or state of integrity of such transactions. This may be the result of various factors such as power failure, improper power supply, malfunction of computer and communication hardware, integrity failures in software programs etc. These lead to the required current state of data not being available, and thus results in the disruption of business services
- ▶ The most common problems of availability occur due to improper capacity availability such as a strangled bandwidth, low computer resources as against the actual requirements such as processing capacity, storage capacity, no. of terminals etc.
- ▶ Intentional damage can also be caused by hackers by denying access to websites or resources using technological means or merely social engineering techniques

Hence, Confidentiality, Integrity and Availability are the basic requirements of Information Security, which need to be safeguarded. The inherent risks of information technology should be understood adequately by the audit professional before attempting to conduct an IS Audit.

Information Systems Risk

Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation.

A significant part of the IS Auditor's work relates to understanding Information Systems Risks and their relationship to controls, thereby understanding the exposure of the organisation to the IS risks. IS Risk Assessment helps the auditor to understand and identify the risks and vulnerabilities and thereby evaluate the state of controls needed to mitigate the impact of such risks.

IS control and audit professionals should possess the expertise to understand and evaluate IS risks and their relationship to business risks. They should also possess the expertise to objectively evaluate the management's risk assessment process and the IS risk profile as determined by the management. This would involve a good understanding of both technology and related management and operational controls that contribute to effective framework controls over management of IS risks.

Understanding IS Risks

The Guidelines for the Management of IT security published by the International Organisation for Standardization (ISO) defines risk as :

“The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. The impact or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated frequency of the threat”

Hence from the above definition, Risk may be inferred to have the following components:

- ▶ Assets or groups of assets that are to be protected
- ▶ Threats that are capable of causing harm to such assets, from which the assets need to be protected, to be assessed taking into consideration the probability of their occurrence.
- ▶ Vulnerabilities that the assets and the safeguards suffer from, which leads to a threat materializing
- ▶ The resulting impact when a threat causes harm to such assets or by exploiting the vulnerabilities thereof

Assets

The first step in risk assessment and management is to identify the subject of the risks, i.e. the assets that need to be protected and assess the level or risk that each asset category is exposed to. In case of Information systems audit it must be appreciated that business processes may be critically dependent on information processes and related information resources. Some category of assets and associated risks are explained below:

Data and Information: Business and related Information contained on various storage devices such as hard disks or in transit over unprotected communication lines may be subject to unauthorized disclosure, copying, theft, corruption or damage.

Application Software: Application software contains the set of instructions that implement the business rules of a business entity. Application software manipulates the data and Information resources to deliver the information requirements of the business users and stakeholders. Such programs may be susceptible to intentional or unintentional unauthorized modification by persons internal or external to the organisation or by faulty technology processes.

Systems Software: Systems software forms the command and control over the computing and communication hardware and provides the necessary platform for operation of application software. Such programs again may be susceptible to intentional or unintentional unauthorized modification by persons internal or external to the organisation or by faulty technology processes.

Module 7, Chapter 1

Hardware and related equipments: The very basis of Information technology is provided by the excellent capabilities of speedy and accurate processing and access capabilities provided by computing equipment such as hardware, devices, peripherals and related equipment. The hardware and related equipments form the basic foundation of the information processing infrastructure. Any harm to the hardware or related equipments could have a critical impact on the information processing capabilities.

Facilities: The computing and communication equipments such as servers could require special environments such as air-conditioned, dust free, humidity controlled facilities. Large data centers are the core of the entire enterprise computing infrastructure. Environmental risks include floods, lighting, earthquakes, tornados, besides fire.

Threats

Computer systems are vulnerable to threats that cause damage – ranging from the loss of database integrity to the destruction of entire computer facilities. The causes of loss could be manifold from mere technological glitches to hackers, disgruntled or adventurous employees, data entry clerks, etc.

An accurate estimate of IS security- related exposures is essential to identify the adequacy of controls as well to estimate the audit planning effort. This is however rather difficult, as some losses remain hidden while others are swept under the carpet to avoid unfavourable publicity. These threats could affect either the confidentiality/integrity of data or their availability of system resources.

A clear idea of threats in the working environment will enable systems managers to implement the most cost effective security measures. They can develop safeguards against threats that exploit the vulnerabilities. If vulnerabilities exist but with a low probability of occurrence, then it may be wiser and more cost effective to simply be conscious about the possibility of such losses and their magnitude rather than implement controls, the costs of which may critically impact the profitability of the enterprise. However this is entirely dependent on the risk appetite of the management. Such decisions would be enabled only by a risk analysis.

People: People are a critical link in making the entire enterprise computing happen. The special skill sets such as IT operational team, programmers, database administrators etc. are a key link in ensuring that the IT infrastructure delivers to the user requirements. Social engineering risks target key persons to get sensitive information to exploit the information resources of the enterprise.

Services: IT computing services are significantly dependent on various vendors and service providers e.g. equipment supply and support, consumables, systems and program maintenance, air-conditioning, hotsite providers, utilities etc.

IS risks are factors that, in some way, harm or reduce operational utility of systems. Threats occur independent of the systems and are a factor that lead to risk. A few common threats are:

Power loss: Power failure can cause disruption of entire computing equipments since computing equipments depend on power supply.

Communication Failure: Failure of communication lines result in inability to transfer data which primarily travel over communication lines. Where an organisation depends on public telecommunication lines, e.g. for e-banking, communication failures present a significant threat that will have a direct impact on operations.

Disgruntled employee: A disgruntled employee presents a threat since, with access to sensitive information of the organisation, he may cause intentional harm to the information processing facilities or sabotage operations.

Errors: Errors which may result from either technical reasons, negligence or otherwise can cause significant integrity issues. A wrong parameter setting at the Firewall to “Allow” attachments instead of “Deny” may result in the entire organisation network being compromised with virus attacks.

Malicious Code: Malicious code such as viruses and worms which freely access the unprotected networks may affect organizational and business networks that use these unprotected networks.

Abuse of access privileges by employees: The security policy of the company authorizes employees based on their job responsibilities to access and execute select functions in critical applications.

Natural disasters: Natural disaster such as earthquakes, lighting, floods, tornado, tsunamis, etc, can adversely affect the functioning of the IS operations due to damage to IS facilities

Theft or destruction of computing resources: Since the computing equipment forms the backbone of information processing, any theft or destruction of a resource can result in compromising the competitive advantage of the organisation

Downtime due to technology failure: IS Facilities may become unavailable due to technical glitches or equipment failure and hence the computing infrastructure may not be available for short or extended periods of

Module 7, Chapter 1

time. However the period for which the facilities are not available may vary in criticality depending on the nature of business and the critical business process that the technology supports

Fire: Fire due to electric short circuits or due to riots, war or such other reasons can cause irreversible damage to the IS Infrastructure

Vulnerabilities

Vulnerabilities are weaknesses in assets or their safeguards that can lead to a threat being materialized. Vulnerability is a condition or weakness in or the absence of safeguards, procedures, technical controls, physical controls or other controls that could be exploited by the threat.

Sometimes the threat viewed in isolation may be misleading unless the vulnerabilities are taken into consideration. In most cases the threats attempt to exploit the vulnerabilities to cause loss or harm to the assets. For example, a hacker would look for loopholes in the architecture of the firewall to compromise the controls and gain unauthorized access to the networks.

Impact

The result of threat that is successful in causing harm or loss to an asset results in an impact. Impact may be either in terms of direct loss of money or financial impact such as a hacker stealing a sensitive file containing all information about credit card customers that is used by the ATM access control system. Impact need not necessarily be in terms of direct impact of money; but can be, for example, disruption of operations leading to operational loss and delayed and back log processing etc. IT risks can also lead to significant losses in terms of damages (both monetary as well as to the reputation of the organization) such as a hacking attack leading to compromising of sensitive financial information of customers, which may be published by the hacker on the Internet resulting in both legal suits by customers and legal repercussions.

IS Risk Assessment

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, reducing it to an acceptable level and maintaining the level or risk. Risk assessment is the process of analyzing and interpreting risk. Risk Assessment consists of following basic activities:

- ▶ Determining the scope and methodology for Risk Assessment
- ▶ Collecting and analyzing data, both quantitative and qualitative
- ▶ Interpreting the risk analysis results

1. Determining the scope and methodology for Risk Assessment

The first step in assessing risk is to identify the environment or system under consideration, the part of the system that will be analyzed, and

the analytical method (including the level of detail and formality) to be adopted.

The assessment could focus on certain areas where either the degree of risk is unknown or is known to be high. Defining the scope and boundary can help ensure cost-effective assessment. Factors that influence scope include:

- ▶ The phase of the life cycle a system is in. More details might be required for a new system being developed, than for an existing system undergoing an upgrade.
- ▶ The relative importance of the system under examination. The more critical the system, the more thorough the risk analysis in terms of decomposing the system into its components and components into its activities
- ▶ The magnitude and types of changes the system has undergone since the last risk analysis. The additional of new interfaces would warrant a different scope than would installing a new operating system

2. Collecting and analyzing data

As seen above, risk has many different components such as assets, threats, likelihood, vulnerabilities and impact. This examination normally includes gathering extensive data about the system under review and synthesizing and analyzing the information relevant to the analysis. Risk Analysis to be reasonably accurate should be significantly data driven. Data would include not only quantitative data but also qualitative data.

As it is possible to land in an undesirable situation of information inundation that needs to be analyzed, planning for risk assessment must ensure the relevance of information to be collected and the methods used therefor. This process is called screening. A risk management effort should focus on those areas that are of the greatest consequence to the organisation (i.e. can cause the most harm). This can be done by ranking assets, threats and controls.

A risk management methodology does not necessarily need to analyse each of the components of risk separately. For example assets/consequences or threats/likelihoods may be analyzed together.

Asset valuation: This includes the information, hardware, software, personnel and facilities. The value of an asset consists of its intrinsic value and the near-term impacts and long term consequences of its compromise.

Impact assessment: Impact assessment estimates the degree of harm or loss that could occur. Impact refers to overall, aggregate harm that occurs, not just the near-term or immediate impacts. While such impacts often result in disclosure, modification, destruction, or denial of service,

Module 7, Chapter 1

consequences are more significant long-term effects, such as lost business, failure to perform the system's mission, loss of reputation, violation of privacy, injury or loss to life. The more severe the impact of the threats, the greater the risk to the system and therefore the enterprise.

Threats identification: A threat is an entity or event with potential to cause harm to the system. As explained earlier, threats include errors, fraud, disgruntled employees, natural disasters, hackers or viruses. Threats should be identified and analyzed to determine the likelihood of their occurrence and their potential to harm assets.

Vulnerability analysis: Vulnerabilities are often analyzed in terms of missing safeguards or weaknesses in safeguards or the very nature of the assets. Vulnerabilities are significant contributors to risk since they may allow a threat or harm to the assets to materialize. The inter-relationship of vulnerabilities, threats and assets is critical to the analysis of risk. However there are other inter-relationships such as the presence of a vulnerability inducing a threat.

Probability or likelihood assessment: Likelihood is the estimation of the frequency, or the chance of a threat happening. A likelihood assessment considers the presence, tenacity and strengths of threats, as well as, the effectiveness of safeguards (or presence of vulnerabilities). In general, historical information about many threats is weak, particularly with regard to human threats; hence the judgment and experience in this area is of relevance. Some threats affect data – especially threats to physical assets such as fires, floods etc. Care needs to be taken in using any statistical threat data; the source of data or the analysis may be inaccurate or incomplete. In general, the greater the likelihood of a threat occurring, the greater the risk.

3. Interpreting Risk analysis results

Risk assessment can support two related functions : the acceptance of risk and the selection of cost-effective controls. To accomplish these functions, the risk assessment must produce a meaningful output that reflects what is truly important to the organisation. Limiting the risk interpretation activity to the most significant risks is another way that the process can be focused to reduce minimize effort and maximize results:

a. Understanding risk assessment

Risk assessment is a process of estimating the potential impact (consequence) that may result from the occurrence of certain threats. Risk assessment is the cornerstone of risk management, which deals with the control measures to minimize these risks. Risk Management is an ongoing process and the primary responsibility for ongoing assessments rests with the management. However for purpose of an independent

evaluation of the risk profile arrived by the organisation, the auditor usually conducts an independent risk assessment.

b. Approach to managing risks

The following table highlights the approach to managing risks:

RISK LEVEL	IMPACT OF RISK AND EXISTING CONTROLS
1	Affects the organisation in a significant manner, but the organisation has no control over the risk e.g. political and economic climate
2	Organisation can exercise some control e.g. regulations and reputation
3	Organisation can monitor and exert significant control e.g. IT risks, people risks and operational risks

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to the management, within applicable constraints. Although risk assessment provides scope for flexibility, the sequence of identifying boundaries, analyzing input and producing an output is quite streamlined. It however depends on the corporate culture and the purpose of risk management activity.

Risk Management is a total process of identifying, measuring and minimizing uncertain events affecting the resources. Risk Management should protect the Confidentiality, Integrity and Availability attributes of Information and Information systems.

Availability – IT resources should be available at a given time and place and in the form required by the user and fundamentally relates to the information and information resources being available when required by the business processes and hence concerns the safeguarding of these resources.

Confidentiality – Access to Information resources should be restricted to a select group of identified individuals or external entities such that the access occurs for authorized purposes and only to the extent necessary. Hence Confidentiality concerns the protection of sensitive information from unauthorized disclosure and access.

Integrity – The business processes should be capable of being performed in a sound, unimpaired manner. Integrity relates to the accuracy and completeness of information and its validity in accordance with the corporate values and expectations.

Understanding the Relationships Between IS Risks and Controls

Understanding the relationship between risk and control is important for an IS Audit. An IS Auditor must be able to identify different types of risks and the related controls used to mitigate such risks.

Risks that threaten the IS cannot be altogether eliminated but, through appropriate decisions and actions that drive security initiatives, can be mitigated. The security measures should be implemented in accordance with the control framework established by the management for Enterprise Risk management. As IS Auditor should evaluate whether available controls are adequate and appropriate to mitigate the IS risks. In the case of deficiency in controls or existence of newer or uncontrolled risks, the IS auditor should report such weaknesses to the auditee management along with appropriate recommendations. Hence it is important for the IS auditor to understand the process and procedure of reviewing and evaluating controls.

IS threats can materialize as an outcome of poor controls or absence of controls. Any threat to the system or its components could result in a loss to the company as a consequence of exploitation of the vulnerabilities. The objective of IS controls is prevent the threats from exploiting the vulnerabilities of the assets or the safeguards. In the event the threats cannot be prevented, the controls should enable timely detection and trigger corrective action. In the event of failure of a control, threats could cause harm to the assets resulting in an actual impact. Exposure refers to the potential loss on account of actualizing of risk. Risk Assessment identifies the elements of risk and combines them to give the overall view of risk.

The risk assessment exercise results in identification of the organisation's risk profile, which is constituted by acceptable risk and residual risk.

Acceptable Risk – Acceptable Risks are risks that organisation recognizes as those that are required to controlled. Management should be conscious that all risks have been identified and where identified, the decision should be taken whether to treat them with controls or not. At the end of the risk assessment exercise, a list of the risks and their “acceptance level” also needs to be documented. However as explained earlier, there may be risks that are beyond the control of the organisation such as risk from fire and risks that the organisation may choose to ignore such as risks from tsunamis etc.

Residual Risk – the remaining risk that is outside the control of the organisation of the risk, or that the organisation does not desire to control is referred to as Residual Risk.

To cite an example, Fire is a threat that can cause significant harm to the data center of an organisation. The susceptibility of the IS resources such as the facilities, hardware, media etc. is an inherent vulnerability. The threat of fire cannot be totally eliminated but however the risk of loss from fire can be mitigated by various technical and control measures e.g. prohibiting smoking within the facility, use of fire proof material for construction of the data center facility, etc. Further, the impact of the loss in the event of fire can be reduced by installing smoke detectors and fire suppression systems, fire proof cabinets etc. Further, the company may obtain an insurance for direct loss (such as destruction of IS assets) as well a loss of profits etc. The choices for treatment of the risk from fire available with the organisation are either to mitigate, transfer, accept or take the extreme step of not going for the data center. The strategy for risk mitigation would vary from organisation to organisation, depending on the risk appetite of the organisation.

The loss that would occur on account of the fire could be termed as exposure. The impact of fire is the actual loss to the organisation due to destruction of assets, disruption of business, loss of customers among others.

One of the common and simple methods of quantification of risks is as follows:

$\text{Risk} = \text{Value of Assets} \times \text{Probability of occurrence of Threat} \times \text{Vulnerability Factor}$

In the above given example let us say the value of Computer equipment is Rs.10,00,000 and the probability of occurrence of Fire is 0.5 and the Vulnerability is increased by 1.5 since the data center is constructed using extensive inflammable wooden materials then the Exposure, in the absence of controls would be

$\text{Exposure} = \text{Rs.10,00,000} \times 0.5 \times 1.5 = \text{Rs.7,50,000}$

However it must be appreciated that Risk assessment is an estimation process that involves quantitative and qualitative estimates.

Controls Assessment

After the risks have been identified, existing controls can be evaluated, or new controls can be designed to ensure that the acceptable level or risk is maintained. When evaluating risks it should be considered whether the controls are preventive or detective, manual or programmed etc.

Controls are defined as “The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.”

Objective of controls

The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. Exposures are potential losses due to threats materializing. All exposures have causes. Some categories of exposures are:

- ▶ Errors or omissions in data, procedure, processing, judgment and comparison
- ▶ Improper authorizations and improper accountability with regard to procedures, processing and judgment and comparison
- ▶ Inefficient activity in procedures, processing and comparison

Some of the critical control considerations in a computerized environment are:

- ▶ Lack of management understanding of IS risks and lack of necessary IS and related controls
- ▶ Absence or Inadequate IS control framework
- ▶ Absence of or weak general controls and IS controls
- ▶ Lack of segregation of duties and job descriptions that reflect the accountability for IS controls
- ▶ Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff
- ▶ Complexity of implementation of controls in distributed computing environments and extended enterprises.
- ▶ Lack of control features or their implementation in highly technology driven environments
- ▶ Inappropriate technology implementations or inadequate security functionality in technologies implemented.

Salient features of controls

The fundamental principles underlying IS control are not entirely different from those of internal controls per se. The fundamental principles have been well laid out in the various Auditing and Assurance Standards issued by the Institute of Chartered Accountants, that can also be extended to apply to Information Systems Controls

- ▶ Management is responsible for maintaining an adequate accounting system, incorporating various internal controls to the extent appropriate to the size and nature of the business. The auditor should reasonably assure himself that the accounting system is adequate, and that all the accounting information, which should be recorded, has been recorded. Internal controls normally contribute to such assurance. (AAS on “ Basic Principles Governing and Audit)
- ▶ The auditor assesses the reliability and sufficiency of the information contained in the underlying accounting records and other source data by:

- ▼ making a study and evaluation of accounting systems and internal controls on which he wishes to rely and testing those internal controls to determine the nature, extend and timing of other auditing procedures... (AAS on Objective and Scope of the Audit of Financial Statements)
- ▶ The system of internal controls extends beyond those matters, which relate directly to the functions of the accounting system. The internal audit function constitutes a separate component of internal control with the objective of determining whether other internal controls are well designed and properly operated (AAS on Study and Evaluation of the Accounting System and Related Internal Controls in Connection with an Audit)

IT Control Objectives

It is the primary responsibility of the management to establish a Risk Management Process. Once the acceptable risks have been identified at every process level, it is now the task of the management to define the Control objectives so as to ensure that the internal controls to control the IS risks are put in place and remain effective. IT Controls objectives seek to ensure that IT remains aligned to business strategies and delivers effectively and efficiently to business requirements, and, in particular, that:

- ▶ the organisation's computing facilities are secure and measures have been taken to ensure continuity of operations
- ▶ the environment ensures completeness and accuracy of data processing
- ▶ information is accessible only to authorized users – secrecy and security of information is maintained
- ▶ effective use is made of computing resources

Defining Control Objectives

Controls are implemented to mitigate risks. Controls always have a cost, but also come with a benefit. The cost could be in terms of time or investment of money. Benefits could be in terms of reduction of risk, or in terms of improving the effectiveness and efficiency of operations. In any organisation, it is crucial to balance the cost vs. benefits of controls. To do this, it is important that controls should not be implemented merely for sake of controls, but should have a specific purpose. The objective of the putting in place the control is termed as control objective. Control Objectives define what is sought to be accomplished by implementing the control and the purpose thereof.

Control Objective is defined as “A statement of the desired result or purpose to be achieved by implementing control procedures in particular IT process or activity”. One of the most important steps in an IS audit is

Module 7, Chapter 1

to identify the control objectives. The control objectives serve two main purposes:

1. Outline the policies of the organisation as laid down by the management
2. A benchmark for evaluating whether control objectives are being met

Category of Controls

Controls are classified in a number of ways. Based on the objective with which controls are designed or implemented, controls can be classified as:

Preventive Controls: Controls that are designed to prevent an error, omission or malicious act from occurring. For example, use of access control software that allows only authorized personnel to access sensitive files and processing options.

Detective Controls: Controls that detect an error, omission or malicious act that has occurred and reports the occurrence. For example, an access violation log that contains the details of access that have taken place. Such features are common in most access security systems software.

Corrective Controls: Controls that correct errors, omissions or malicious acts once they are detected. For example, the clean option of an anti-virus program that is programmed to immediately delete malicious codes and scripts once they are detected, before the code can cause damage. Correction controls also help mitigate the losses where the threats have impacted the assets thus helping in reducing the intensity of the impact.

Another classification of controls is based on the nature of such controls with regard to the nature of IS resources to which they are applied:

- ▶ **Environmental Controls-** Controls relating to facilities provided for housing IT resources such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc.
- ▶ **Physical Access Controls** – Controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, video monitoring etc.
- ▶ **Logical Access Controls** – Controls relating to logical access to information resources such as Operating systems controls, Application software boundary controls, networking controls, access to database objects, encryption controls etc.

- ▶ **IS Operations Controls** – Controls relating to IS operation, administration and its management such as day begin and day end controls, IS Infrastructure management, Helpdesk operations etc.
- ▶ **IS Management controls** - Controls relating to IS management, administration, policies, procedures, standards and practices, monitoring of IS operations, Steering committee etc.
- ▶ **SDLC Controls** – Controls relating to planning, design, development, testing, implementation and post implementation, change management of changes to application and other software

Further another category of controls is based on their functional nature. A well designed computer system should have built-in controls for all its major functions. In addition , the auditor should understand the basic control objectives of all applications at a given time. The internal control systems components could include:

- ▶ **Internal accounting controls** – Controls that are primarily directed at the transaction accounting operations that deal with safeguarding assets and the reliability of financial records.
- ▶ **Operational controls** – Controls that are concerned with day to day operations, functions and activities that ensure that operations are meeting the business objectives and adherence to business rules
- ▶ **Administrative controls** – Controls that are concerned with operational efficiency in any functional area and adherence to management policies and procedures. These controls can be described as supporting the operational controls, specifically for ensuring efficiency and cost effectiveness of operations.

Mitigating IS Risks Through IS Risk Management

Like any other risk, IS Risks cannot be absolutely reduced to nil. Hence the strategy lies in mitigating the risks to an acceptable level. Hence the importance of fixing the Acceptable level of risks i.e. the level of risks, considering the entire profile of risks, that the management considers needs to be controlled. Therefore, it is important for the management, as well as the IS auditor conducting the Risk assessment, to arrive at the Risk profile which would consist of the acceptable risks as well as the residual risks. A systematic Risk assessment process for identifying, qualifying and quantifying the IS resources is a critical precursor to effective risk management.

Risk Management is increasingly accepted as the core to any organisation's strategic management. The process involves systematic addressing of risks attached to various processes and activities with the goal of achieving sustained benefit within each activity thereby leading to the effective achievement of business objectives. Information Systems Risk management should form an integrated part of the organisation's

Module 7, Chapter 1

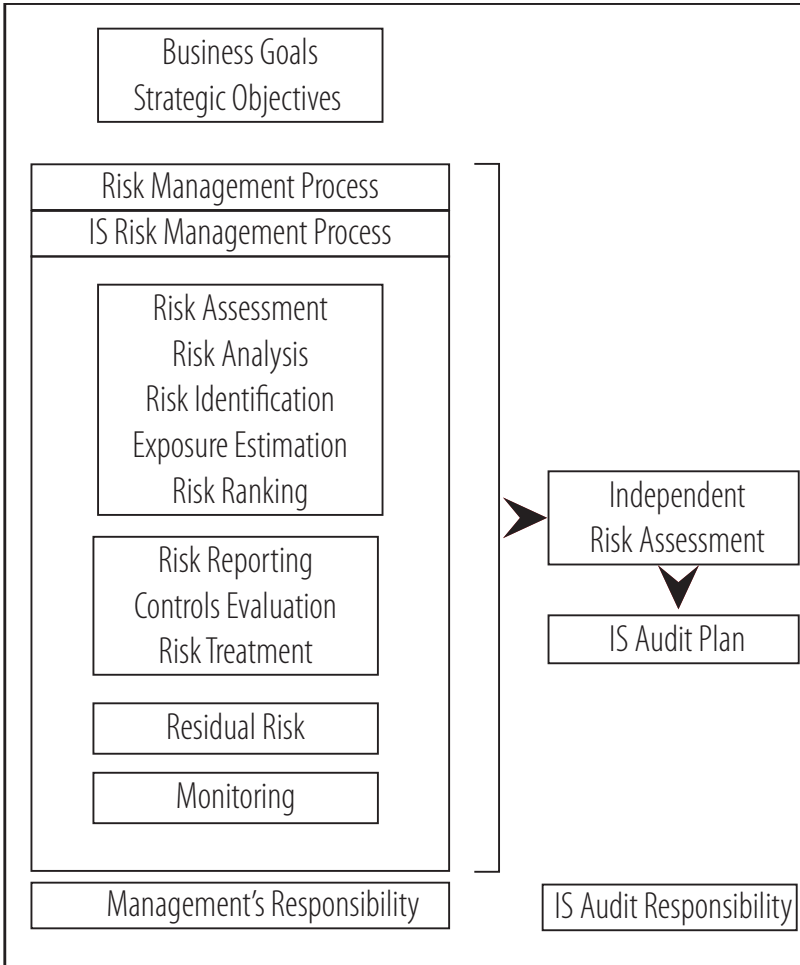
Business Risk Management process. IS risk management should form a key consideration of all major business initiatives. A critical aspect is the need for ongoing risk management, monitoring and review. The selection of appropriate methodology is a key factor, which may vary from organisation to organisation.

Similar to general business risk management, IS risk management also deals with potential for events and consequences that constitute opportunities for benefit or threats to success. An effective information resource risk management program identifies the key information resources used by the enterprise. It assigns primary responsibility for information protection to the top management and once the support and commitment of top management is secured, the roles and responsibilities are fixed on the executive management responsible for management of every functional area. The business managers and not the IT management are the right persons towards vetting the design and implementation of the IS Risk management program since they are aware of the nuances of the business risks in operational areas under their control and are in a better position to assess the impact of undesirable events. They are also a position to decide the level of delegation of authority and access levels that can be given to other users. For example, the Sales and Marketing Department is in a better position to decide on the degree of rights with regard to access to Sales and Marketing data and related processing resources by other User Departments.

IS Risk management should be an on-going and continuous process which runs throughout the organisation's strategy and the implementation of the strategy. IS Risk management contributes to the organisation's strategy and adds value to the organisation and stakeholders through supporting the organisation's objectives by:

- ▶ Providing a framework of IS Risk assessment
- ▶ Enabling better business planning and strategic alignment between business and IT that results in decision making, planning and direction being achieved in a structured manner with best results.
- ▶ Leading to efficient utilisation of the organisation's IS resources and accounting for its usage by both internal as well as external stakeholders
- ▶ Reducing deployment of resources in wasteful and unproductive projects
- ▶ Ensuring security of the IS resources
- ▶ Optimising Operational efficiency
- ▶ Supporting future orientation and learning initiatives to lead to continuous process improvement

Risk Management and Audit Planning



Role of Auditor in Risk Assessment

The Auditing and Assurance Standard on “ Basic principles governing an audit” requires that:

“The auditor should first gain a clear understanding of the accounting system and related internal controls. He should study and evaluate the operation of internal controls that he wishes to rely on to determine the nature and timing and extent of other procedure.

If the auditor concludes that he can rely on certain internal controls, then the substantive procedures will be less extensive than would otherwise be required. IT may also differ in nature and timing.

Module 7, Chapter 1

Further the Auditing and Assurance Standard on “Risk Assessment and control” requires that

“The auditor should obtain an understanding of the control environment sufficient to assess directors’ and managements’ attitudes, awareness and actions regarding control and its importance in the entity. Further the standard also states that the internal control environment may be affected by, among others the organisation structure. Therefore, it will be appropriate to look at the organizational aspects first.”

The internal control appraisal should focus only on the risks that exist and the controls required. Best practices may also have evolved with time and the auditor should keep these in mind.

Computers have affected the way organisations process their data. They can also influence internal control, making traditional control techniques ineffective and sometimes even eliminate the need for them. Control techniques and the placement of controls may change with computers but the objective does not change. For example, the objectives of internal control in a financial accounting system are broadly related to:

- ▶ Transaction authorization
- ▶ Transaction recording
- ▶ Access to assets
- ▶ Accountability and comparison

Internal controls evaluation

Internal control refers to any policy, procedure or activity that serves to safeguard assets, maintains the accuracy of financial data, improves operational efficiency and enforces adherence to management policies. The data reflected in the financial statements is a result of the internal control systems.

Identification of control weaknesses is an inherent part of every IS audit and involves:

- ▶ Assessing conditions, their causes and effects
- ▶ Gathering reliable evidence to support such assessments

Internal control includes:

- ▶ Information systems and the plan of the organisation
- ▶ Methods adopted by the management that ensure orderly and efficient conduct of its business
- ▶ Policies for safeguarding the assets, prevention and detection of fraud and error, accuracy and completeness of the accounting records and the timely preparation of reliable financial information

Evaluating the adequacy of internal accounting and operational controls is the central core around which traditional auditing involves. The evalu-

ation of controls in the case of Information Systems Audit is not entirely different. However the IS auditor should have a clear understanding of the IS audit objective and scope. IS Audits can vary from evaluation of controls relating to specifically financial transactions alone or extent to evaluation of controls vis-à-vis operations such as the controls in an ERP environment. The IS auditor may be required to even specifically evaluate the technical controls relating to the IS Infrastructure. Even in the case of an IS Audit of accounting systems, the auditor should be in a position to identify the control weaknesses arising from technical reasons which could significantly impact the accounting controls e.g. internal entries triggered within ERP software. Hence there is a need for the internal control framework to integrate the technical controls and their impact on the business controls, and the audit should document, process, summarise and report on the state of controls.

Most audit engagements should include an evaluation of internal controls either directly as part of the audit objectives, or as a basis to rely upon information being gathered as part of the risk assessment phase of the audit. Where the objective is focused on evaluation of internal controls, the auditor should distinguish between the types of engagements.

Internal controls are a key area, which need to be evaluated a part of the audit whether it is internal IS audit or external IS audit. In case of a computerized environment, it must be appreciated that the internal controls are built as part of the application software and other related software itself. Business rules validation, checks and balances, authorizations, validations, and access levels are logically built into application software, which will need to be evaluated.

Hence it is important for the auditor to include the evaluation of controls based on the audit objective as part of his preliminary assessment and audit planning phases. The auditor would need to decide on the use of Computer aided audit techniques such as use of generalized audit software that enable effective and efficient evaluation of controls with regard to their existence, reliability and compliance, that would need to be tested as part of the audit plan.

Audit Considerations in Case of Outsourced IT Activities

Outsourcing of IS activities to an external service provider is a common practice in most organisations. The activities that can be outsourced include IS operations management, IS infrastructure management, application systems development, maintenance and the like.

Often the risk management as regards outsourced IT activities is weak or not considered within the purview of the IS infrastructure at all. It is

Module 7, Chapter 1

not unlikely that the audit charter may not cover the outsourced activities.

The expectations and requirements as regards the service and service levels are usually laid out in the contracts and agreements with the service provider. However there may exist significant ambiguity in terms of such agreements and contracts.

The auditor should:

- ▶ ascertain all the IT processes and activities that have been outsourced and have access to the contracts and agreements
- ▶ understand the nature, timing and extent of outsourced activities, where the IS auditor is assigned the audit of any particular IT process or underlying activities.
- ▶ define the roles and responsibilities as regards the input dependencies and service delivery and performance
- ▶ identify the risks associated with the outsourced activities
- ▶ identify the controls that have been established by the service provider to ensure that the services are provided as per the agreed terms
- ▶ assess whether the controls are reasonable and assure that the services will be provided as per the terms of the agreement and undesired events will be either prevented or detected and corrected
- ▶ determine whether the agreement provides for audit of the outsourced services.

Audit Planning

Before commencing his audit work, as part of the preliminary review, the auditor should review the previous audit reports. He should also consider the policies on service level agreements and third party service contracts. The auditor should also gain an understanding of the constitution, stability, operating environment and history of the service provider. The existence of the right to audit clause is an essential pre-requisite before the auditor can proceed to audit the outsourced activities with regard to the service provider.

Audit performance

During the course of audit, the auditor should ensure that a service level framework is in place as part of the Risk management and control framework of the auditee organisation. The service level agreements with the outsourced services provider should be in compliance with the policies and procedures defined as part of the service level framework. The IS auditor should also review the minutes of meetings and discussion between the auditee and the external service provider. The auditor should conduct audit procedures to determine compliance with the quantitative and qualitative provisions of the agreements.

The auditor should ensure that the following form a part of the service level agreement:

- ▶ Service provider should comply with all legal requirements that are applicable to the outsourced service activity.
- ▶ Should provide for a right to audit clause and requirement of control responsibilities.
- ▶ Responsibility of the service provider to establish performance monitoring procedures
- ▶ Business continuity measures to be put in place to ensure continuity of service
- ▶ Non disclosure requirements as regards information and processes of the auditee organisation handled and control stipulations in this regard
- ▶ Insurance requirements.

The auditor should conduct audit procedures to evaluate the performance measurement which should require that:

- ▶ Measurement mechanisms be set in place and metrics be agreed upon.
- ▶ Service delivery should meet the minimum quality attributes as agreed or generally applicable
- ▶ Benchmarking of the services of the service provider with those of the competitors or industry practices
- ▶ Penalties and Liquidated damages where the service levels fall below agreed levels.

Information Systems Control Framework

The plethora of risks that arise with the use of IT and the newer risks that the use of IT creates for business need to effectively managed. However managing the business risks from use of IT is often more complex than what it appears. An organisation's effective IT Risk management is not merely putting up firewalls or other sophisticated technologies but is a complex combination of both technical and human controls in the right proportion. Controls, if too complex and involving, can be a competition risk e.g. enforcing an Internet banking user to change his PIN number every 30 days. Security that has significant overhead on functionality can impact business adversely. At the same time lack of poor controls and lack of education of customers on security practices can also lead, for example, to increased credit card frauds, which again will wean away the business to the competitor. Hence taking the IT control and security of the enterprise as a whole would require an orchestrated set of security technologies, control policies, procedures and practices to be put in place throughout the organisation.

Hence evolving an Information Systems Control Framework is as effective only with a systematic and structured approach to Information

Module 7, Chapter 1

Security, primarily driven by the Information Risk Assessment process. A few of the critical requirements for evolving an Information Systems Control Framework include:

1. Top Management understanding and support for Information Security as a prime business concern.
2. Top Management to allocate adequate budgets for Information Security both in terms of money and human resource
3. Organisation wide awareness and understanding of Information as a key business resource that must be protected.
4. Inventorying and classifying information assets.
5. Establishing an effective Risk Management Process aligned with business strategy, as a continuing effort
6. Identify technologies and related enabling resources in use from a risk perspective and the control objectives, including but not limited to:
 - a. Security of Personnel
 - b. Physical and Environmental Security
 - c. Management of networks and related communication technologies
 - d. Identity Management and Access Control
 - e. Controls over Systems Development and Maintenance
 - f. Business Continuity Planning
7. Establishing an Organisation Structure and fixing accountability for Information Assets
8. Appointing a top level, highly representative governing forum with centralized responsibility for all strategic IS security initiatives and operations
9. Enhancing enterprise wide IS security awareness and training staff on a continuing basis
10. Independent monitoring mechanism for Information Risk Management

The result of the above should translate into an effective Control Environment, usually through the Enterprise wide Security Policy.

Security Policy Framework

The policies and procedures supported by the standards, baselines, guidelines and security technologies together form the Security Policy Framework. The security policy framework seeks to provide meshed controls using technical and importantly human controls, which is often the weak link in any organisation. The policies and procedures are the critical components of the Control Environment that lay down the requirements regarding information security requirements. The legal and regulatory requirements, industry requirements, agreements, IT

Control and security standards etc. should be considered while drawing up the Security Policy.

A good security policy should clearly state the following:

- Purpose and Scope of the document and the intended audience
- The basic security requirements and the security infrastructure
- Security Policy Structure, Security Policy document maintenance and compliance requirements
- Incident Response Mechanism and Incident Reporting
- The security organisation structure
- Inventory and classification of assets
- Description of technologies and computing architecture
- Policies as regards Outsourcing and Third party access
- Personnel Security and related HR policies
- Physical and Environmental Security
- Identity Management and Access Controls
- IT Operations management
- IT communications
- Systems Development and Maintenance Controls
- Business Continuity Planning
- Legal and Compliance Requirements
- Monitoring and Auditing Requirements
- Underlying technical policy

IT Governance

The Bank of International Settlements defines “governance arrangements to encompass the set of relationships between the entity’s management and its governing body, its owners and its other stakeholders, and providing the structure through which:

- the entity’s overall objectives are set
- the method of attaining those objectives is outlined and
- the manner in which performance will be monitored is described”

With enterprises significantly dependent on Information technology, IT is gaining its role as a business driver from a mere business enabler, hence there is need for strategic alignment of IT with the business strategy, the expectations of the stakeholders from information technology need to be clearly defined and performance needs to be measured to determine whether IT is meeting the expectations, management needs to whether Information technology is adding value and whether the IT resources are being utilized efficiently and above all whether the risks from IT are managed effectively.

The IT Governance Institute defines IT Governance as:

“a structure of relationships and processes to direct and control the enterprise in order to achieve its enterprise’s goals while adding value while balancing risk versus return over IT and its processes”

Module 7, Chapter 1

The following are excerpts from the Board Briefing on IT Governance issued by the IT Governance Institute:

Successful enterprises understand the risks and exploit the benefits of IT, and find ways to deal with:

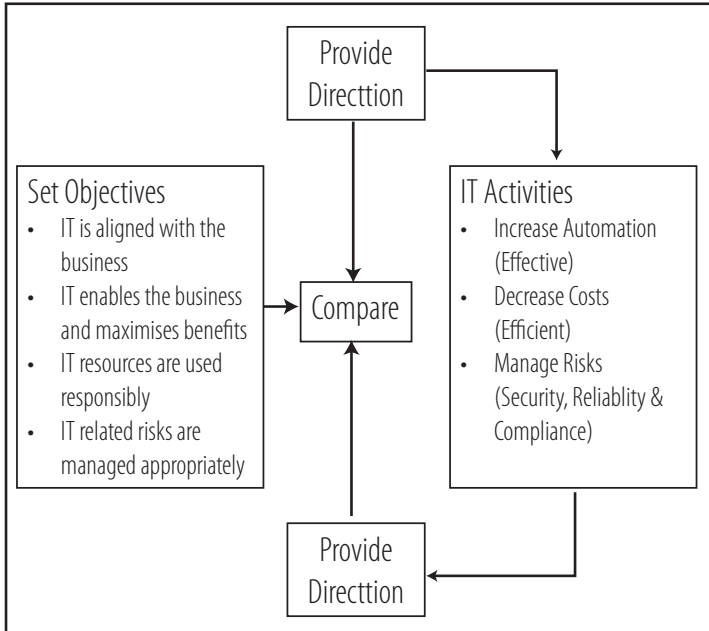
- ▶ Aligning IT strategy with the business strategy
- ▶ Cascading IT strategy and goals down into the enterprise
- ▶ Providing organisational structures that facilitate the implementation of strategy and goals
- ▶ Creating constructive relationships and effective communications between the business and IT, and with external partners
- ▶ Insisting that an IT control framework be adopted and implemented
- ▶ Measuring IT's performance

Boards and management need to assess their capacity to:

- ▶ Take advantage of IT's enabling capacity for new business models and changing business practices
- ▶ Balance IT's increasing costs and information's increasing value to obtain an appropriate return from IT investments
- ▶ Manage the risks of doing business in an interconnected digital world and the dependence on entities beyond the direct control of the enterprise
- ▶ Manage IT's impact on business continuity due to increasing reliance on information and IT in all aspects of the enterprise
- ▶ Maintain IT's ability to build and maintain knowledge essential to sustain and grow the business
- ▶ Avoid the failures of IT, increasingly impacting the enterprise's value and reputation

The overall objective of IT governance, therefore, is to understand the issues and the strategic importance of IT, so that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. IT governance aims at ensuring that expectations for IT are met and IT risks are mitigated.

IT Governance Focus



Hence the focus issues for IT Governance are:

- ▶ IT Strategic Alignment – Aligning IT with business strategy
- ▶ Value Delivery – Optimising IT expenses and making IT deliver business value
- ▶ Risk Management – Addressing the IT risks, safeguarding IT assets and minimizing disruption to business from IT.
- ▶ Performance Measurement – Measuring the performance of IT to business against pre-determined expectations from IT
- ▶ Resource Management – Managing the IT resources and infrastructure and optimising knowledge

Appendix 1: Sample E-mail Security Policy

I. Introduction And Purpose

- A. This Policy clarifies the applicability of law and of other organisational policies to electronic mail (e-mail), and also sets forth new policies uniquely applicable to e-mail.
- B. The Organisation recognizes that principles of academic freedom, freedom of speech, privacy and confidentiality hold important implications for e-mail and e-mail services. This Policy addresses these principles within the context of and subject to the limitations imposed by the Organisation's legal and policy obligations.

Module 7, Chapter 1

The purpose of this Policy is to assure that:

1. E-mail will be used by the Organisation's employees in an ethical and considerate manner in compliance with applicable law and policies, including policies established by the Organisation and its operating units, and with respect for the public trust through which these facilities have been provided;
2. E-mail users are informed about how concepts of privacy and security apply to e-mail, as well as the applicability of relevant policy and law; and
3. Disruptions to Organisation e-mail and other services and activities are minimised.

II. Application Of Other Policies

All policies applied generally at the Organisation are expressly applicable to the electronic environment.

III. Scope

A. This Policy Applies to:

1. All e-mail services provided, owned, or funded in part or in whole by the Organisation;
2. All users and holders of Organisation e-mail systems or accounts, regardless of intended use; and
3. All Organisation e-mail Official Records and/or Public Records in the possession of or generated by Organisation employees and other users of e-mail services provided by the Organisation, regardless whether the records were generated on Organisation or non-Organisation computers.

B. This Policy does not apply to:

1. Internet services other than e-mail;
2. Voice Mail;
3. Audio and Video Conferencing; and
4. Facsimile messages.

C. This Policy does not apply to printed copies of e-mail, but other law and policy may apply to such documents.

D. This Policy applies equally to transmission and receipt data including e-mail headers, summaries, and addresses associated with e-mail records and attached files or text.

IV. Specific Use Provisions

A. Provision of Service

E-mail services may be provided by organizational units in support of the Organisation's threefold mission of instruction, research, and public service.

B. Organisation Property

E-mail services are extended for the sole use of Organisation faculty, staff, students and other appropriately authorized users to accomplish tasks related to and consistent with the Organisation's mission. Organisation e-mail systems and services are Organisation facilities, resources and property as those terms are used in Organisation policies and applicable law. Any e-mail address or account assigned by the Organisation to individuals, sub-units, or functions of the Organisation, is the property of the Organisation.

C. Authorized Service Restrictions

1. E-mail users are required to comply with state and federal law, Organisation policies, and normal standards of professional and personal courtesy and conduct. Access to Organisation e-mail services is a privilege that may be wholly or partially restricted by the Organisation without prior notice and without the consent of the e-mail user: a) when required by and consistent with applicable law or policy; b) when there is a reasonable suspicion that violations of policy or law have occurred or may occur; or c) when required to meet time-dependent, critical operational needs. Such access restrictions are subject to the approval of the appropriate Organisation supervisory or management authority (e.g., department heads, systems managers, etc.). The autonomous operational units of the Organisation should establish or identify these authority levels.
2. Organisation operational units may define additional "Conditions of Appropriate Use" for local computing and network facilities to supplement this Policy with additional detail, guidelines or restrictions. Such Conditions must be consistent with and subordinate to this Policy, and are intended to deal primarily with situations of limited resource supply.
3. When an individual's affiliation with the Organisation ends, the Organisation may attempt to redirect e-mail for a reasonable period of time as determined by the Organisation for purposes consistent with this Policy and the Organisation's mission. The Organisation may elect to terminate the individual's e-mail account or continue the account, subject to approval by appropriate Organisation supervisory and systems operational authority.

D. Authorized Access and Disclosure.

1. The Organisation may permit the inspection, monitoring, or disclosure of e-mail when:
 - a. Required by or consistent with applicable law or policy
 - b. There is a reasonable suspicion that violations of law or Organisation policy have occurred or may occur; or

Module 7, Chapter 1

- c. There are time-dependent, critical operational needs of Organisation business if the Organisation determines that the information sought is not more readily available by other means.
2. In such instances, the Organisation will, as a courtesy, normally try to inform e-mail users prior to any inspection, monitoring, or disclosure of e-mail records, except when such notification would be detrimental to an investigation of possible violation of law or Organisation policy. Users are required to comply with Organisation requests for access to and copies of e-mail records when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the Organisation. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate Organisation personnel policies or Codes of Conduct.

E. Indemnification of the Organisation.

Users agree by virtue of access to the Organisation's computing and e-mail systems, to indemnify, defend and hold harmless the Organisation for any suits, claims, losses, expenses or damages, including but not limited to litigation costs and attorney's fees, arising from or related to the user's access to or use of Organisation e-mail and computing systems, services and facilities.

V. Misuse

- A. Using e-mail for illegal activities is strictly prohibited. Illegal use may include, but is not limited to: obscenity; child pornography; threats; harassment; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; attempting to intercept any electronic communication transmissions without proper authority; and violation of copyright, trademark or defamation law.
- B. Failure to follow state law with regard to the disposition of e-mail records may lead to criminal charges. Theft or unauthorized destruction, mutilation, defacement, alteration, falsification, removal or sequestration of e-mail records may lead to violation of the Information Technology Act.
- C. In addition to illegal activities, the following e-mail practices are expressly prohibited: entry, examination, use, transfer, and tampering with the accounts and files of others, unless appropriately authorized pursuant to this policy; altering e-mail system software or hardware configurations; or interfering with the work of others or with Organisation or other computing facilities.
- D. If a user has been requested by another user via e-mail or in writing to refrain from sending e-mail messages, the recipient is prohibited from sending that user any further e-mail messages until such time

as he/she has been notified by the system administrator that such correspondence is permissible. Failure to honor such a request shall be deemed a violation of this Policy.

- E. Organisation e-mail services may not be used for: commercial activities not approved by appropriate supervisory Organisation personnel consistent with applicable policy; personal financial gain (except as permitted under applicable academic policies); personal use inconsistent with Section VI of this policy; uses that violate other Organisation policies or guidelines; or uses inconsistent with applicable state or federal law. Applicable Organisation policies include, but are not limited to, policies and guidelines regarding personnel, intellectual property, or regarding sexual or other forms of harassment.
- F. E-mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements of behalf of the Organisation or any unit of the Organisation unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of the Organisation."
- G. Organisation e-mail services shall not be used for purposes that could reasonably be expected to cause, directly, or indirectly, strain on any computing facilities, or interference with others' use of e-mail or e-mail systems. Such uses include, but are not limited to, the use of e-mail services to:
 - 1. Send or forward chain letters.
 - 2. "Spam", that is, to exploit listservs or similar systems for the widespread distribution of unsolicited mail.
 - 3. "Letter-bomb", that is, to resend the same e-mail repeatedly to one or more recipients.

VI. Personal Use

Organisation e-mail services may be used for incidental personal purposes provided that such use does not:

- A. Directly or indirectly interfere with the Organisation operation of computing facilities or e-mail services.
- B. Interfere with the e-mail user's employment or other obligations to the Organisation.
- C. Violate this Policy, or any other applicable policy or law, including but not limited to use for personal gain, conflict of interest, harassment, defamation, copyright violation or illegal activities.
- D. E-mail messages arising from such personal use shall, however, be subject to access consistent with this policy or applicable law. Accordingly, such use does not carry with it a reasonable expectation of privacy.

VII. Confidentiality

- A. The confidentiality of e-mail cannot be assured, and any confidentiality may be compromised by access consistent with applicable law or policy, including this Policy, by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access. Users, therefore, should exercise extreme caution in using e-mail to communicate confidential or sensitive matters, and should not assume that their e-mail is private or confidential.
- B. Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information, regardless whether the information is maintained on paper or whether it is found in e-mail or other electronic records.

VIII. SECURITY AND PRESERVATION

- A. E-mail users and operators must follow sound professional practices in providing for the security of e-mail records, data, applications programs, and systems programs under their jurisdiction.
- B. Users and operators must guard against storage media deterioration and e-mail record inaccessibility due to hardware or software obsolescence. To eliminate these situations, users must make provision for future accessibility by:
 - 1. Migrating all official e-mail records to the next generation of hardware or software; or
 - 2. Migrating only current official e-mail records to new hardware or software, or converting official e-mail records not migrated to other media (e.g., optical disk, COM) for short term storage or to "eye readable form" (i.e., paper or microfilm) for long term storage and preservation.
- C. Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized. Each user is responsible for all e-mail transactions made under the authorization of his or her ID, and for all network e-mail activity originating from his or her data jack. Use of e-mail user identifications for commercial purposes is prohibited. Access to user identifications may not be loaned or sold.
- D. Each operational unit should establish:
 - 1. Standards for official e-mail records identification and file organization.
 - 2. Measures for protecting sensitive official e-mail stored electronically.
 - 3. Procedures for file back-up.

IX. VIOLATIONS

Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs. Violations will be processed by the appropriate Organisation authorities and/or law enforcement agencies. Violations may result in revocation of e-mail service privileges; academic dishonesty or Code of Conduct proceedings; faculty, staff or student disciplinary action up to and including dismissal; referral to law enforcement agencies; or other legal action.

X. ON-LINE POLICIES

Users of this Policy are encouraged to refer to on-line versions of this and other Organisation policies when available on the Organisation's home page on the World Wide Web.

Appendix 2: Sample Control Objectives for Logical Security of Operating System

A. Understanding Systems

Organisation

To ensure that the audit team has a clear understanding of the delineation of responsibilities for system administration and maintenance.

Hardware Platforms

To ensure that the audit team has a clear understanding of the hardware platforms subject to review and to obtain the necessary information for identifying critical systems throughout the processing environment.

To ensure that the audit team has a clear understanding of the operating system included in the scope of the review. Furthermore, to ensure that known vulnerabilities associated with specific operating system versions are considered during the audit.

Network Overview

To ensure that the audit team has a clear understanding of network components and interfaces, which may affect the logical security of specific servers and workstations.

B. Security Management

Roles and Responsibilities

To ensure that roles and responsibilities for security management have been clearly and appropriately defined.

Corporate security policies and standards

To ensure that existing corporate security policies and standards have been communicated. Furthermore, to ensure that existing policies and standards are applicable throughout the processing en-

Module 7, Chapter 1

vironment and that all systems are in compliance with appropriate policies and standards.

Security Awareness and Training

To ensure that end-users are aware of appropriate corporate security policies and standards and are informed of their individual responsibilities for a secure processing environment.

C. Security Administration

Roles and Responsibilities

To ensure that roles and responsibilities for security administration have been clearly and appropriately defined.

Staffing

To ensure that appropriate processes are in place, and individuals with security administration responsibilities are qualified to perform their tasks.

Security Administration Procedures

To ensure that security administration responsibilities and activities have been adequately defined and documented to support the security administration function, and to ensure that appropriate documentation is available to facilitate training processes for new administrators.

D System Configuration

Servers

To ensure that adequate controls are in place for the installation and configuration of server hardware.

Operating System Configuration - policies and standards

To ensure that operating system installations and upgrades are configured in compliance with appropriate security and configuration policies and standards.

Operating System Configuration - configuration process

To ensure that adequate controls are in place for the configuration of operating system installations and upgrades.

Operating System Configuration - system security parameters

To ensure that existing operating system security parameters are configured to secure settings and are in compliance with best practices and relevant corporate policies and standards.

System Utilities

To ensure that adequate controls are in place over the use of sensitive system utilities.

Security System Configuration - policies and standards

To ensure that third-party security system installations and upgrades are configured in compliance with appropriate security and configuration policies and standards.

Security System Configuration - configuration process

To ensure that adequate controls are in place over the configuration of third - party security system installations and upgrades.

Security System Configuration-system security parameters

To ensure that existing parameters for third-party security systems are configured to secure settings and are in compliance with best practices and relevant corporate policies and standards.

E. Access Controls

Account Management

To ensure that appropriate controls are in place for the system level account management process.

Password Management

To ensure that the system has been configured to facilitate the use of secure passwords to prevent unauthorized access to critical applications, data and system resources.

User Profile Configurations

To ensure that adequate controls are in place for the configuration of user profiles to ensure that user access rights are commensurate with users' job responsibilities.

Group Profile Configurations

To ensure that adequate controls are in place for the configuration of group profiles to ensure that access rights for users assigned to the group profiles are commensurate with users 'job' responsibilities.

Privileged Accounts

To ensure that adequate controls are in place for the authorization, ownership and use of sensitive super- user accounts.

Special User Accounts

To ensure that appropriate controls are in place for the logon and logoff processes.

Logon / logoff processes

To ensure that appropriate controls are in place for the logon and logoff processes.

Generic / Shared accounts

To ensure that the use of generic and shared accounts is limited and justified by business need and to ensure that appropriate controls are in place over the use of these activities.

Remote Access

To ensure that appropriate controls are in place to control access to the internal network and systems from a remote system.

System Boot Process

To ensure that appropriate controls are in place to ensure that only authorized security settings and system services are initiated during the system boot/IPL process.

F. File & Directory Protection

System Directories and Files

To ensure that system level security has been configured to appropriately protect critical system directories and files.

Applications Directories and Files

To ensure that system level security has been configured to appropriately protect critical application directories and files.

Production data, directories and files

To ensure that system level security has been configured to appropriately protect critical production data directories and files.

G Reporting and Auditing

Logging

To ensure that appropriate security events are logged to provide security administration personnel with the ability to appropriately monitor system security.

Reporting

To ensure that appropriate reports are produced to summarise data recorded in audit logs so that security events may be efficiently monitored on a timely basis.

Monitoring

To ensure that appropriate processes and procedures are in place to monitor security reports in order to detect security violations and unauthorized changes to system security configurations in a timely manner.

Summary

IS audit fundamental objectives include verification of safeguarding of assets, integrity of data, effective achievement of organizational goals and efficient use of IT resources. It is necessary for IS auditors to have expert understanding of risks in a computerized environment, with focus on the triad of confidentiality, integrity and availability, besides the productivity and compliance expectations. With the dynamic nature of IS risks, this requires a continuous process of risk assessment and controls adjustment being in place to ensure the achievement of business objectives in the expected manner. As part of the risk assessment, the risks associated with their protection from threats and as a result of vulnerabilities are critical to the work of the auditor. Based on the risk profile, the adequacy of controls need to be verified to ensure that the acceptable risks have been appropriately controlled. With a plethora of risks and the intricacy of controls, consisting of manual and programmed procedures, effective security would require a framework approach to risk management. At a broader level, an IT Governance approach is essential for the organisation to ensure that IT delivers to the business objectives and does not present with surprises.



2 Overview of Information Systems Audit

✂ Learning Goals ✂

To gain an overview of the entire IS audit process,

Impact of Information Technology on the Audit

While the fundamental objectives of auditing may not have changed, IT has impacted the manner in which the audit objectives would be achieved in a computerized environment.

Information processing has always been a part of the business requirements hence Information processing per se is not something new. However Information Technology makes a clear difference in enabling the information processes as regards transaction processing, in terms of speed, accuracy, and reach

The impact of IT on the audit function can be understood with attention to the nature of changes that IT has brought about, some of which include:

- ▶ IT has moved from a mere enabling tool used for achieving accounting, sales or payroll processing activities to driving enterprises using Enterprise Resource Planning solutions and Extended Enterprises. This has led to crushed transaction cycle times with computers completing a single transaction spanning various stakeholder systems. This has also led to a more competitive environment as a result of the need to act fast and to a need for appropriate business strategies kindled by the very nature of Information Technology.
- ▶ Transaction cycles such as purchase, sales etc. can be almost entirely automated with business rules being driven by application software
- ▶ Internal controls as regards transaction, accounting and operational controls are embedded in the technology environment, which are automatically executed as part of the instruction sets that drive transaction rules.
- ▶ Networking has dissolved boundaries with trade now capable of being carried out irrespective of transacting parties being located on even the most diverse locations on the globe.
- ▶ E-commerce has eliminated the need for physical meeting or even presence of transacting parties, and introduced the concept wherein

Module 7, Chapter 2

trade cycles, that can be entirely initiated and completed by two connected systems across the globe.

Besides the positive traits, the use of Information Technology for businesses has also introduced several newer risks and concerns:

- ▶ Errors in software and program codes can introduce financial and non financial impact of catastrophic proportions
- ▶ Information Technology comes with its set of risks such as risk of unauthorized logical access to sensitive business information, Risks such as cyber crimes, virus attacks etc.
- ▶ Dependence on IT for business also results in adverse impacts due to the inherent risks of computing and communication infrastructure of failure and breakdown.
- ▶ With increasing technology enablement, understanding and managing the complex IT controls is becoming a nightmare.

Given the above situation, the impact on auditing can be understood to be two fold:

- a. Traditional audit techniques either almost invariably will fail to achieve the traditional audit objectives whether it be external financial audits or internal audits, or the cost of audits and the time required would be unjustifiably higher. This can be also referred to as Auditing in a computerized environment
- b. The emergence of newer risks due to introduction of information technology and the very inherent nature of risks that IT suffers from, has also introduced the need for assurance on related security and controls. This can be referred to as conducting an IT Audits.

Need for IS audit

Computers have had a profound effect on both the nature and the manner in which business is done or service is rendered. Information Technology that integrates computers and telecommunication technology has revolutionized the way business is done and has created new models of business and delivery of goods and services. IT is not merely a tool for business information processing but is now looked upon as a business driver and pertinent to the success and survival of business. Even smaller organisations are realizing the competitive advantage that IT can enable and have experienced phenomenal growth with the use of Information Technology. With customers and stakeholders also realizing the benefits of computers, enterprises as well as individuals have become critically dependent on information technology to achieve their day to day activities.

However, the inherent risks that Information technology suffers from has introduced newer risks to business. The methods of implementing internal controls have undergone a significant change with the increas-

ing use of IT. Businesses now realize Information Technology as a strategic risk, affecting the control needs:

- ▶ Need for control over errors and omissions, which can cost the organisation significant losses
- ▶ Need for control over computerization since improper/lack of controls in application software and related information technology can lead to incorrect business decisions.
- ▶ Need for control over abuse of information technology resources by persons both external and internal to the organisation
- ▶ Need to ensure IT controls are so designed as to protect against legal, financial and non-financial risks arising from IT risks
- ▶ Need to assure that the IT risks are well managed and that IT is aligned strategically with the business requirements and that IT resources are well managed.

IT has always been viewed as a technology issue alone and not one with potential impact on business. Business managers seldom understand the need of their involvement in designing, developing and implementation of information systems. Information technology experts are generally not equipped with intrinsic knowledge of business controls and internal controls. As a result only when disasters and disruptions happen to business due to IT, does it result in the top management's realization of the nature of impact that IT can have on the business. Hence there is an increasing realization amongst the business management and users that technology is not merely the IT department's subject but a critical enterprise wide business concern. Hence there is need for an independent assurance function that is equipped with the knowledge of Information Technology Risks, the controls to manage such risks and to assure the IT and the Business management that IT risks are managed appropriately. Chartered Accountants who are acknowledged experts in business controls and audit when equipped with the requisite Information technology and related controls knowledge are the obvious choice for filling the requirement.

Control techniques and the placement of controls may change with the introduction of computers, but the objectives are likely to remain the same. Traditional controls, such as segregation of duties, dual control and accuracy verification, are now replaced by application controls within computer programs.

But incompatible duties that must be segregated still exist. For example, the duty of developing a design for a software application must be segregated from that of writing program codes. This segregation means that the designer and the programmer have to collude to perpetrate a fraud which is difficult. In addition, having two persons performing different

activities of the same process provides with the necessary checks and balances to prevent any misuse.

Definition of IS Audit

Ron Weber in his book *Information Systems Control and Audit* defines Information Systems auditing as

“ the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organisation goals to be achieved effectively and uses resources efficiently.”

Another definition, defines Information Systems audit as an audit that encompasses review and evaluation (either wholly or partly) of automated information processing systems, related non- automated processes and the interfaces between them.

These definitions provide a broad overview of the objective and tasks involved in an Information systems audit. However IS audit is a special audit assignment which is done by competent and specially trained staff, who may be either internal to the enterprise or done by an external professional agency. The objective and scope of coverage of IS audit is usually defined by the management but sometimes there may be situations where the IS auditors may be called upon to do an independent risk assessment to determine the scope of the engagement.

Scope of IS Audit

Based on controls to be reviewed, IS audit broadly involves testing and assuring on the following controls:

- ▶ IT Control Framework – This includes the IT policy and strategic integration of IT and related general controls in the Control framework
- ▶ Organisational controls – include controls relating to segregation of incompatible IT activities
- ▶ Logical access controls – Controls implemented through systems and application controls
- ▶ Application Controls – Controls built into application software
- ▶ Physical Access controls – Controls relating to securing the physical access to facilities and IT resources
- ▶ Environmental Controls – Controls relating to specific environmental control requirements of sensitive IT equipment and technology
- ▶ IS operations controls – Controls relating to day to day operations of Information Systems
- ▶ SDLC Controls – Controls relating to design, development, testing and implementation of application and systems software
- ▶ Business Continuity Controls – Controls relating to business continuity and disaster recovery

Objective of IS audit

An IS audit is expected to provide reasonable assurance to the management on the quality (effectiveness, efficiency, and economy), protection against internal and external IT risks (Confidentiality, Integrity and Availability) and fiduciary (compliance and reliability) perspectives of Information and related technology. IS auditors help their clients to understand and manage IT risks. It enables IT organisations to use leading edge technology and stay ahead in a competitive environment by implementing business and process oriented controls. The scope of IS audit is defined by the auditee organisation based on specific needs.

IS auditing involves the evaluation of systems and procedures to ensure that assets are safeguarded : the integrity of computer data is maintained, and the objectives of the organisation are achieved. The objective of the IS audit is to determine if all control procedures for computer systems are in place, and to identify any areas where control can be improved. Both these functions will reduce potential losses.

The IS audit is designed to evaluate the adequacy of internal controls with regard to both specific computer programs and the data processing environment as a whole. This includes evaluating both the effectiveness and efficiency. The focus (scope and objective) of IS Audit is not only on security which comprises confidentiality, integrity and availability but also on effectiveness (result-orientation) and efficiency (optimum utilisation of resources).

Effectiveness refers to the accomplishment of the objective. An inventory system can be developed either using manual controls or using a computer system. But if the volume of inventory is large, it may become a tedious, potentially erroneous, costly and time-consuming process. Still the method is considered effective as long as the ultimate objective of completing the process and delivering the relevant information on time is accomplished. Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

Efficiency refers to the accomplishment of the objective in the shortest time, at the optimal cost. For example, a program could create records either on tape or disk files. As long as the daily creation of these records does not take up too much time, both approaches would be considered equally efficient. However, if the records were to begin to consume three or more tapes or files, then the measurement of efficiency will change. The tape system will no longer be as efficient as the disk system because it would take significantly more processing time to post the records to the tape file than it would to the disk file. Efficiency focuses on providing the information through the optimal (most productive and economical) usage of resources.

The importance of processes and activities that should be subjected to audit would be based on an objective risk assessment and hence a Risk based audit approach. Only items that need to be considered on priority with regard to risk management would ideally be considered as part of a Risks and Controls assurance audit.

Fundamentals for Establishing an IS Audit Function

Establishing an IS audit function may be critical in organisations that are critically dependent on Information Technology. IS audit function could be either established either within and as an internal department of the organisation or the function could be fully or partly outsourced to an external agency. In either case there are certain fundamental principles that should be taken into consideration:

- ▶ **Audit Charter** – A charter is the top level document that formally recognizes the audit function having the approval of the senior management. The document clearly defines the responsibility, authority and accountability for IS audit function.
- ▶ **Structure and Reporting of the IS audit function:** The IS audit function should be so placed in the organisation so as to ensure its objectivity and independence. The appointment of external agency should also be governed by stipulations for independence and objectivity, which is the foundation for an effective audit function. The composition and constitution of the IS audit function should ideally be decided by the Audit Committee and should be the prime reporting pointer for the IS Audit function.
- ▶ **Staffing the IS Audit function:** Another important determinant in the quality of the IS audit function is the quality of Human resource that staff the audit function. The skills and competence requirements should be clearly established and as an IS Audit function should collectively possess the skills and knowledge necessary for performing an effective and professional audit. Even in cases where external agencies are engaged, the professional competence and skills of such agencies should be ensured. Continuing Professional Education should be ensured as part of the IS audit management plan.
- ▶ **Internal and External Audit Control Framework:** To ensure minimum quality of audits, it is important for the organisation to ensure setting in place an Audit Control Framework. Policies and procedures for risk assessment, planning, implementation and Reporting should be established. The standards and professional pronouncements should be strictly adhered to, which should be reflected in the organisation and operations of the audit function.
- ▶ **Quality Assessment and Peer Reviews:** To ensure that the IS audit function is delivering in line with the best auditing practices and following the professional standards and pronouncements, the IS Audit

function should be subject to both internal and external quality assessments, peer reviews, certification and accreditation.

Audit Mission

The mission statement defines the primary purpose of the audit function. It also outlines the value addition that will be provided. The mission statement provides an overview of the focus, priorities, values and principles that will measure audit decisions. It also guides and clarifies the purpose and meaning for the audit function. The audit mission statement may vary between various organisations and audit functions.

An example of the audit mission statement is given below:

The mission of the audit function is to provide value added services in auditing and consulting by timely effective and efficient processes, encompassing all key business processes of the enterprise so as to facilitate achievement of business objectives.

Audit Charter

The audit charter is a top level document in an organisation that defines the purpose of the audit function, responsibility and authority and reporting of the audit function. The audit charter is approved by the senior management.

A charter for the audit function should be established by the senior management of the organisation. This document should outline the responsibility, authority and accountability of the audit function. It should be reviewed periodically to assure that the independence, authority and accountability of the audit function are maintained.

Management should ensure that the auditors responsible for the review of the organisation's IT activities are technically competent and collectively possess the skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner. Management should ensure that audit staff assigned to an IS audit and technically competent and participate in continuous professional education

The IS auditor should have a clear mandate to perform the audit. This mandate is generally documented in an audit charter and endorsed by the management.

The audit charter should clearly address three aspects: responsibility, authority and accountability.

Responsibility

- ▶ Mission Statement
- ▶ Aims/Goals
- ▶ Scope
- ▶ Objectives
- ▶ Independence

Module 7, Chapter 2

- Relationship with External audit
- Auditee requirements
- Critical success factors
- Key performance Indicators
- Other measures of performance

Authority

- Risk Management
- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope of limitations to scope
- Functions to be audited vs. auditee expectations
- Organisational structure, including reporting lines to the board and senior management
- Grading of IS audit staff

Accountability

- Reporting guidelines to senior management
- Assignment performance appraisals
- Personnel performance appraisals
- Staffing/career development
- Auditee's rights
- Independent quality reviews
- Assessment of compliance with standards
- Benchmarking performance and functions
- Assessment of completion of the audit plan
- Comparison of budget with actual costs
- Agreed actions, e.g. penalties when either party fails to carry out its responsibilities

Communication with Auditees

Effective communication with auditees involves:

- Describing the service, scope, availability and timeliness of delivery
- Providing cost estimates or budgets, if they are available
- Describing problems and possible resolution
- Providing adequate and readily accessible facilities for effective communication
- Determining the relationship between the service offered and the needs of the auditee

The audit charter should be the basis for communication with auditees and should include references to service level agreements on the following aspects:

- Availability for unplanned work
- Delivery of reports costs
- Response to auditee complaints

- ▶ Quality of service
- ▶ Review of performance
- ▶ Communication with auditees
- ▶ Needs Assessment
- ▶ Control risk self assessment
- ▶ Agreement on terms of reference for audits
- ▶ Reporting process vs. agreement of findings

Example of an audit charter

Every auditee organisation should have an approved charter (mandate, mission statement) describing the audit function's purpose, authority, scope and responsibilities. It should include statements relevant to the IS auditing function. An example of an IS audit charter is given below:

- A. **Purpose:** IS audit is an independent appraisal activity. Its main objective is to conduct computer systems and operations review and report findings and recommendations to management and others
- B. **Authority:** The audit function will have full, free and unrestricted access to all the organisation's activities, functions, records, property and personnel necessary for achieving its objectives. The audit function is a staff function and is responsible for reviewing computer related activities and reporting findings and recommendations. However it does not have authority over or the responsibility for these activities. Also, the audit function cannot relieve any manager of the requirement of ensuring proper control within his or her area of concern.
- C. **Scope and responsibilities:** IS Audit should provide assurance to the management that the controls which govern computer systems and operations are properly conceived and effectively administered. When ineffective, inefficient or uneconomical practices are identified during an audit, suggestions should be made to the management that will improve control over its computer systems and operations.

Engagement Letter

Purpose

Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between the external IS auditor and an organisation.

Content

The engagement letter should clearly address the three aspects – responsibility, authority and accountability

Responsibility

- ▶ Scope

Module 7, Chapter 2

- Objectives
- Independence
- Risk Assessment
- Specific Auditee requirements
- Deliverables

Authority

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment
- Scope or any limitations to the scope
- Evidence of agreement to the terms and conditions of the engagement

Accountability

- Intended recipients of reports
- Restrictions on distribution
- Auditee's rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

Skills and Competence Requirements of an IS Auditor

The overall competence level required for an IS depends on the nature, complexity and size of IS audit engagement. The audit objective and scope would have a significant bearing on the skill and competence requirements of an IS auditor. However a set of skills that is generally expected of an IS auditor include:

- Sound knowledge of business operations, practices and compliance requirements
- Should ideally possess the requisite academic, professional and technical qualifications and certifications
- A good grasp of Information Systems Risks and Controls
- Knowledge of Information and related technology control framework.
- Knowledge of IT strategies, policy and procedure controls
- Ability to understand the IT environment of the auditee
- Good knowledge of Information Technology concepts and working knowledge, to the extent necessary for the engagement, including hardware, operating systems, database management systems, networking technologies, information technology architectures etc.
- Ability to understand systems design, development, implementation and project management concepts
- Understanding of technical and manual controls relating to Business Continuity

- ▶ Good communication skills and the ability to highlight the business issues arising from IT risks
- ▶ Good knowledge of Regulatory requirements and Laws relating to Information Technology controls and cyber crime
- ▶ Good knowledge of Professional Standards and Best practices relating to IT controls and security

Any IS audit assignment begins by defining the scope and objectives. Based on this, the auditor should obtain a clear understanding of business operations, compliance requirements, technology deployed, organisation structure, related risks of technology deployment and system of internal controls. He could then adapt the standards and benchmark for audit, develop an information model for collecting and evaluating evidence and execute the audit.

Illustrative List of IS (Review) Audit and Consulting Services

A. Review of Consulting on Environmental and Physical Security

This review covers controls over the IT process of managing facilities, especially with regard to the environment and physical security. It is expected to provide assurance to the management that the process of environment and physical access to IT resources are appropriately controlled and monitored. It should satisfy the business requirements of providing a suitable physical environment, which protects the IT equipment and people against man-made and natural hazards.

This review broadly considers the systems and procedures (relating to the installation of suitable environmental and physical controls. It also confirms whether they are regularly reviewed and functioning effectively. The specific areas evaluated are:

- ▶ Access to facilities
- ▶ Site identification
- ▶ Physical security
- ▶ Inspection and escalation policies
- ▶ Business continuity planning and crisis management
- ▶ Personnel health and safety
- ▶ Preventive maintenance policies
- ▶ Environmental threat protection
- ▶ Automated monitoring

B. Review Or Consulting On Logical Access Security

This review covers control over the IT process for ensuring systems security, specifically with regard to logical access. It should provide assurance to the management that the processes that are in place for granting access to system satisfy the business requirements of safeguarding in-

formation against unauthorised use, disclosure or modification, damage or loss.

This review address issues related to the implementation of application program mechanisms. It involves the evaluation of controls over the IT process, and ensures that the system security safeguards information against unauthorised use, disclosure, modifications, damage or loss. This review broadly considers whether there are appropriate logical access controls, which ensure that access to systems, data and programs is restricted to authorised users. The specific areas evaluated are:

- Confidentiality and privacy requirements
- Authorisation, authentication and access control
- User identification and authorisation profiles
- Need-to-have and need-to-know
- Cryptographic key management
- Incident handling, reporting and follow-up
- Virus prevention and detection.
- Firewalls and centralised security administration
- User training and tools for monitoring compliance, intrusion testing and reporting.

C. Review and Consulting on IT Enterprise and Relationship

This review addresses issues that are pertinent to the creation of an appropriate organisational structure that will oversee and administer the information services function. It broadly considers whether the organisation has adequate staff with appropriate competency and skill-sets. It verifies whether their roles and responsibilities have been appropriately defined and communicated, aligned with the business objectives. The specific areas evaluated are:

- Board IT responsibility levels
- Management direction and IT supervision
- IT alignment with the business
- IT involvement in key decision processes
- Organisational flexibility
- Balance between supervision and empowerment
- Job descriptions, staffing levels and key personnel
- Organisational positioning of security, quality and internal control functions
- Segregation of duties.

D. Review or Consulting on Application Software and Data Security.

This review covers control over the IT process of managing and protecting data. It is also expected to provide assurance that appropriate and

adequate controls are available in the application software deployed at the enterprise. They should ensure that data is complete, accurate and valid during its input, update and storage.

This review addresses issues that are pertinent to the establishment of proper data preparation procedures-minimizing errors and omissions. It broadly considers whether there is effective combination of application and general controls over the IT operations. The specific areas evaluated are:

- Form design and source document controls
- Input, processing and output controls
- Media identification, movement and library management
- Data back-up and recovery
- Authentication and integrity
- Data ownership and data administration policies
- Data models and data representation standards
- Integration and consistency across platforms
- Legal and regulatory requirements.

E. Consulting on Identifying Automated Solutions

A consulting assignment assists the management in identifying the right automated solution to satisfy the user requirements. As part of the assignment, clear identification and analysis of the choices against user requirements ought to be done.

Specific areas considered in recommending the right solution are:

- Knowledge of solutions available in the market
- Acquisition and implementation methodologies
- User involvement and buy in
- Alignment with organization and IT strategies
- Information requirements definition
- Feasibility studies (costs, benefits, alternatives, etc.)
- Functionality, operability, acceptability and sustainability requirements
- Compliance with information architecture
- Cost-effective security and control
- Supplier responsibilities

F. Review of Process of Acquisition and Maintenance of Application Software

This review covers controls over the IT process that acquires and maintains application software. It is expected to provide assurance to the management that the application software (sought to be acquired or already acquired), and the maintenance process will provide automated functions, which effectively support the business process. The broad areas covered here are : making clear specific statements of functional and

operational requirements, and ensuring phased implementation with clear deliverables. The specific areas evaluated are:

- Functional testing and acceptance
- Application controls and security requirements
- Documentation requirements
- Application software life cycle
- Enterprise information architecture
- System development life cycle methodology
- User-machine interface
- Package customisation.

G. Review or Consulting on Business

The review covers control over the IT process of ensuring continuous service. It is expected to provide assurance that IT services will be available as required and business impact in the event of a major disruption is minimised.

This review also addresses IS issues related to the adoption and implementation of procedures that ensure continuity of service in the event of a disaster. It broadly considers whether the organisation is having an operational and tested IT continuity plan in line with the overall business continuity plan and its related business requirements. The specific areas evaluated are :

- Criticality classification
- Alternative procedures
- Back-up and recovery
- Systematic and regular testing and training
- Monitoring and escalation processes
- Internal and external responsibilities of an organisation
- Business continuity activation, fallback and resumption plans
- Risk management activities
- Assessment of single points of failure
- Problem management

H. Review or Consulting on IT Strategic Planning

This review covers the IT process of defining a strategy. It should provide assurance that the IT strategic planning process has struck a fine balance between IT business opportunities and business requirements.

This review broadly considers the development of long-term plans based on the strategic planning process. The long-term plans are then periodically translated into short-term goals (i.e. operational plans)

The specific areas evaluated are :

- Enterprise business strategy
- IT support to business objectives
- Inventory of technological solutions and current infrastructure

- Monitoring the technology markets
- Timely feasibility studies and reality checks
- Existing systems assessments
- Enterprise position on risk, time-to-market, quality
- Need for senior management buy-in, support and critical review.

Summary

Extensive computerization of operations in user organizations has made IS audit mandatory. The Chapter starts with defining what constitutes IS audit and explains the why of it. Then it goes on provide an overview of the IS audit - the important preliminary activities such as defining scope and objective to drafting audit mission and charter. To a traditional financial auditor, the question uppermost in his / her mind is what are the additional skills and competencies required to conduct an IS audit, which is detailed here. An illustrative list of activities is provided to aid the auditor in practice.



3 Information Systems Audit Performance

✂ Learning Goals ✂

To understand how an IS Audit is planned and carried out, viz. IS Audit Strategy, Phases in Information Systems Audit, Planning an IS audit, Use of Sampling in Information Systems Audits, Documentation Requirements, Reporting and Follow Up

Information Systems Audit Strategy

Information Systems Audit is often misunderstood as a mere technical audit and a domain of Information Technology professionals. On the contrary, Information Systems Audit involves evaluating the adequacy of internal controls and business controls in business processes that are either partly or fully computerized. Hence Audit and control professionals who have expertise in understanding of business controls and internal controls with exposure to information technology controls are considered the most appropriate professionals to conduct most information systems audits.

An Information Systems Audit cannot be viewed from a narrow perspective of audit of only automated information processing systems but would include audit of non-automated processes and interfaces.

Therefore, depending on the audit environment, objectives and scope, the audit could involve audit of entire business processes, which may be automated in part or full or could require audit of specified application, technology and related controls.

The audit strategy would also be influenced by a range of factors, some of which include:

- ▶ **Type of audit:** Information systems audit could involve testing of controls relating to business controls and internal controls ingrained in IT systems or controls relating to technology risks. The audit objectives could be quite diverse e.g. from an enterprise wide information systems audit as regards testing for security, quality and compliance issues of focused only on testing of security of a particular area.

Information Systems Audit may be required by any statute such as The Information Technology Act, 2000, Sarbanes Oxley 2002 or by regulations such as directives and regulations of the Reserve Bank of India. On the other hand audits and assurance reviews could also be driven by

Module 7, Chapter 3

certification requirements such as the BS 7799 or required by the management as a self evaluation of IT and related controls.

- ▶ The audit strategy would also be significantly influenced by the following:
 - ▼ Nature and Complexity of business
 - ▼ Extent of automation
 - ▼ Risk Profile of the business and technology environment
 - ▼ Complexity of technology environment
 - ▼ Degree of controls
- ▶ **Audit environment:** The nature of business, the technology environment, control framework and culture etc. would have a significant bearing on the audit strategy. For example the audit strategy for a business of trading in securities which involves high transaction risk would be further impacted from the extent of automation. The securities broking firm could be connected to the Stock Exchange and Depositories Systems whereby significant risks relating to the controls would be believed to be taken care of by the business and related internal controls implemented using technology controls.
- ▶ **Competence and skill requirements :** Depending on various factors, the audit strategy should consider independence and objectivity requirements, special skills that may be required to conduct the audit, use of Computer Aided Audit techniques and generalized audit software etc.

Phases in Information Systems Audit

Information Systems Audit could broadly be understood of comprising of various sets of activities, which can be divided into the phases given below. Each phase normally results in information which could be used for the subsequent phase. Each of the phases involve detailed activities required to achieve the objectives of the phase.

The phases in Information Systems Audit can be divided as follows:

- ▶ Preliminary Review of Audit Environment
- ▶ Agreement on objectives and scope of audit
- ▶ Planning the audit assignment
- ▶ Audit Procedures
- ▶ Reporting
- ▶ Follow Up

While each of the phases would follow in order, some phases may be eliminated or taken in a different order, depending on other considerations e.g. The phase of preliminary review of audit environment would be more elaborate in the case of the first information systems audit to determine the objectives and scope, which may not be required in case

of routine audits, in which case the preliminary review is taken up as part of the planning phase.

Planning an IS Audit

One of the primary and important phases in an Information Systems Audit is planning which ensures that the audit is performed in an effective manner. Planning takes on more significance in case of Information Systems Audit since audit risk in case of IS audits are significantly impacted by inherent risks, hence for the audit effort to be successful, a good audit plan is a critical success factor.

As per IFAC, “Planning” means developing a general strategy and a detailed approach for the expected nature, timing and extent of the audit. The auditor plans to perform the audit in an efficient and timely manner.

Planning the Information Systems Audit involves numerous activities and a range of considerations and would be impacted by the objective and scope and preliminary review of the audit environment.

As per ISA 300 on “Planning”:

- ▶ Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, that potential problems are identified and that the work is completed expeditiously. Planning also assists in proper assignment of work to assistants and in coordination of work done by other auditors and experts.
- ▶ The extent of planning will vary according to the size of the entity, the complexity of the audit and the auditor’s experience with the entity and knowledge of the business.
- ▶ Obtaining knowledge of the business is an important part of planning the work. The auditor’s knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
- ▶ The auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity’s audit committee, management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity’s personnel. The overall audit plan and the audit program; however, remain the auditor’s responsibility.

The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the auditor.

Module 7, Chapter 3

The audit should be guided by an overall audit plan and underlying audit programs that guide the course of the all audit activities. Audit planning is often mistaken as a one time activity to be taken and completed in the beginning of the audit. Planning is a continuous activity throughout the period of audit, this is because changes in conditions or unexpected findings and results may throw new light requiring change in the premise audit, resulting in modifications required in the audit procedures.

The documentation of the audit plan is also a critical requirement. All changes to the audit plan should follow a change management procedure with every change being recorded with reason for change.

Preliminary Review

The extent of audit effort is dictated by the degree of audit risk, the assessment of which is critical to the effectiveness of the audit effort. Amongst the critical factors affecting the audit risk is the appropriate assessment of the control environment. The preliminary review of enables the auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit.

As per ISA 300 on “Planning”, matters to be considered by the auditor in developing the overall plan, the following are some of the critical factors to be considered by the auditor as part of his preliminary review that would provide critical inputs for the planning exercise:

Knowledge of the Business

- ▶ General economic factors and industry conditions affecting the entity’s business.
- ▶ Important characteristics of the entity, its business, its financial performance and its reporting requirements including changes since the date of the prior audit.
- ▶ The general level of competence of management.

Understanding the Technology

An important task for the auditor as part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- ▶ Extent of computerisation of business processes
- ▶ Extent of dependence of the enterprise on Information technology to carry on its businesses
- ▶ Technology architecture which could be quite diverse such as a distributed architecture against a centralized architecture or a hybrid architecture
- ▶ Extended enterprise architecture wherein the organisation systems connects seamlessly with other stakeholders such as vendors, customers and the government .

- ▶ Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems
- ▶ Information Technology policies, procedures, parameter settings, standards, manufacturer specifications etc.

Understanding the Accounting and Internal Control Systems

- ▶ The accounting policies adopted by the entity and changes in those policies.
- ▶ The effect of new accounting or auditing pronouncements.
- ▶ The auditor's cumulative knowledge of the accounting and internal control systems and the relative emphasis expected to be placed on tests of control and substantive procedures.

Legal Considerations and Audit Standards

The auditor should carefully evaluate the legal as well as statutory implications on his audit work.

- ▶ The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
- ▶ The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organisation. Sometime this may also include restrictions on the use of certain types of technologies e.g. strength of encryption systems .
- ▶ The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

Risk and Materiality

- ▶ The expected assessments of inherent and control risks and the identification of significant audit areas.
- ▶ The setting of materiality levels for audit purposes.
- ▶ The possibility of material misstatement, including the experience of past periods, or fraud.
- ▶ The identification of complex accounting areas including those involving accounting estimates.

Nature, Timing and Extent of Procedures

- ▶ Possible change of emphasis on specific audit areas.
- ▶ The effect of information technology on the audit.
- ▶ The work of internal auditing and its expected effect on external audit procedures.

Module 7, Chapter 3

As mentioned earlier, generally in the case of the first information systems audit of a part of whole of the enterprise, the client may not be in a position to clearly define the objectives and scope of audit. In such a case the auditor may be called upon to conduct a preliminary review of the audit environment with respect to the basic requirement of the client to enable fixing the audit objective and scope. In this case the objectives and scope of the audit may not be known at the beginning and hence planning for audit can be taken up only after agreement on the objective and scope of audit.

The preliminary review of audit environment would involve the following:

- ▶ **Evaluation of business requirements:** The IS auditor should consider the focus area for review, the business requirement and nature of information and its relation to the business processes. This stage requires the auditor to gain an understanding of the nature of business, the business processes and the related information processing architecture.
- ▶ **Evaluation of the technology environment:** Based on his understanding of the business and business process, the IS auditor proceeds to gain an understanding of the technology environment that supports the information processing requirements of the organisation. This activity requires the auditor to have knowledge of the various information technology architectures and their impact on the business controls.
- ▶ **Evaluation of control environment:** Based on his understanding of the business and related information technology environment, the IS auditor proceeds to evaluate the control framework which comprises of the business strategy, IT strategy, organisation structure, policies and procedures. This activity would assist the IS Auditor in understanding the Information systems resources and the controls over such resources. Here the IS Auditor should have competence in evaluating the impact of controls and the absence thereof in a technology driven environment, that are strategic to the enterprise. As a part of this activity, the IS Auditor should also gain a good understanding of the types of transactions, business and related technology events that impact on the business and related processes and functions of the organisation. Based on the understanding gained in the preceding activities, the IS Auditor should be in a position to identify the impact on his audit work and related support and actions required of the management. At the stage the IS auditors should also identify activities relating to Information systems development or processing activities that are outsourced to external service providers.

Audit Charter and Engagement letter

The audit may be either done by an IS Auditor or IS audit department of the company or a part or the whole of the function may be outsourced to an external independent professional IS audit firm or agency.

In either case, the audit charter, which contains the mandate for the audit function should be considered. Where an audit function internal to the organisation is available, the audit charter would clearly spell out the responsibility, authority and accountability of the audit function and also specify the existence of a Service level agreement between the audit function and the management and users.

Where Information systems audit is outsourced to an external agency, an engagement letter often issued for every assignment, the terms of which should be considered at the time of planning.

Agreement on Audit Objectives and Scope

Information Systems audits could involve either the audit of information and related systems of the entire enterprise or focused audit on certain application or technology areas.

Information Systems audit objectives may be quite diverse, such audit may be either required by the statute or regulatory authority or required for purposes of certification against accepted security standards and models or required by the management as part of internal evaluation of information systems controls.

Broadly Information systems audits target the following attributes of information:

- ▶ **Security** – which is broadly comprised of confidentiality, integrity and availability of information and information systems.
 - ▼ **Confidentiality** refers to the risks relating to unauthorized disclosure or access to the information assets
 - ▼ **Integrity** refers to the risks relating to unauthorized modification to the state of the information assets.
 - ▼ **Availability** refers to the risks relating to the information assets not being available or not being available in the manner so as to enable the efficient discharge of the business activities.
- ▶ **Quality**
 - ▼ Relates to how effectively information systems and technology deliver to the expected requirements
 - ▼ Relates to how efficiently the information systems and technology are utilized to deliver to the expectations

Module 7, Chapter 3

► **Compliance**

- ▼ Refers to whether the information systems and technology deliver to the requirements of the external legal, regulatory or other compliance requirements or internal business compliance requirements.

In every case, the audit team (may be internal or external to the organisation) and the management should clearly understand, define and agree upon what is required and what the audit will deliver.

It is important to define the scope and objectives of the assignment and the area or coverage, which would be spelt out as part of the terms or reference. Audit scope could be defined based on the selection of relevant IT processes or resources or information criteria (security, quality or compliance).

In the case of audits required by any statute or regulations, the objectives and scope of audit would usually be spelt out as part of the rules or guidelines underlying such statute (e.g. the audit of Certifying authorities under the Information Technology Act 2000). The scope as regards area to be covered and locations to be covered may be spelt out as part of the terms of reference.

The auditors may have to play a key role in assisting the management in the fixation of objectives and scope, criteria and extent of coverage etc. Before proceeding with the audit, a clear agreement on the above should be obtained.

Risk Assessment

One of the key steps during the planning stage is Risk assessment. Risk assessment is used to risk profile of organisation or the area and related controls. The degree or risk would determine the audit effort required hence risk assessment is a key to planning and extent of testing with respect to the audit. It must also be remembered that Risk assessment is primarily a task of the management and on-going in nature. The audit function's role is only to independently evaluate the risk profile assessed by the management. The auditor may also come across situations, where the organisation may not have any risk assessment process in place, in which case, the auditor would need to take significant care in arriving at the risk profile.

While there some guidelines on risk assessment, various risk assessment methodologies are used which may vary with respect to the type and nature of audit. The auditor would have to evolve a suitable strategy and methodology for risk assessment. As discussed in detail in the section on "Risk Assessment" separately, risk is a complex derivative of the value of information assets, threat profile and vulnerabilities.

Every organisation would naturally have put in place a significantly complete set of controls to counter the risks. However the auditor would have to evaluate the adequacy of such controls and also identify the risks that are either consciously left out (residual risks) and more importantly the risks that have escaped the management's attention. While doing an information systems audit, the auditor must understand and be competent to appreciate the impact of inherent risks, which have a significant impact on the risks and controls.

Most managements/audit departments perform some type of risk analysis that varies from sophisticated software driven models to pure subjective judgments. Whether based on highly data driven objective or subjective methods, the gaps in controls and areas of high risk are identified for audit.

A risk analysis model, which is usually a collection of complex mathematical models with various subjective interpretations, is generally used. Such models involve computation of numeric scores which are arrived based on numeric ratings assigned to various factors such as criticality of asset, severity of threat, and vulnerability. However it is important that such methods do not get lost in granular details which may lead to waste of effort with not so significant contributions towards the final result. Hence whatever models are adopted should be simple and workable and help to reasonably arrive at the most prudent risk profile. However it is not possible to arrive at a standard model or methodology which can be directly applied across organisations, hence every organisation would need to have its own risk analysis methodology and model. A good risk model should consider all the various factors such as appropriate valuation criteria for assets, method of classification and evaluation of threats and vulnerabilities, consider the various types of controls such as entity level controls, general management controls, general IT controls and application controls.

Internal Controls Evaluation

Identification and classification of risks to information assets is only a precursor to controls evaluation. Once the information assets are inventoried, classified and relevant risks are identified, the next important task is the evaluation of the design of controls that have been put in place. The efficacy of such controls should further be considered in terms of their nature such as preventive, detective and corrective, level of organisation at which such controls are designed, approved, applied and monitored.

Evaluation of internal controls is an inherent part of most Information Systems Audits, this may be either directly required to be done as part of the audit or required indirectly as part of the audit objectives. The audit may require either evaluation of the effectiveness of controls at a par-

Module 7, Chapter 3

ticular point of time or over a period of time, and the audit procedures should be appropriately designed to meet the objectives.

It is the responsibility of the management, as part of putting in place a control framework, to identify control activities and determine control objectives to be achieved with respect to all critical information resources. The auditor should identify and independently evaluate such control objectives and based on his evaluation, relate them to the audit objectives.

The auditor normally makes a preliminary evaluation of controls to arrive at a basis for developing the audit plan. During such process the auditor should consider audit procedures to test the reliability of the stated controls and provide for leeway in modifications to the audit plan.

Various techniques are available for the overall evaluation of internal controls. Auditors need to adapt those that are most suitable or relevant for the audit. Some of these techniques are:

- ▶ Impact assessment based on the severity of impact on the organisation with respect to various factors such as strategic, financial, internal operations, reputation, stakeholder interests etc.
- ▶ It is appropriate to assign suitable ratings based on the adequacy of controls such as Good, Adequate, Inadequate and Poor. Numeric ratings are popular such as assigning the evaluation of controls based on say 1-5 with “5” representing poor or no controls and “1” representing good controls. The objective is to assess the adequacy and quality of internal controls based on the management/auditor’s knowledge. If control weaknesses exist in a particular area, the score will be higher. A poor rating represented by a high numeric score then reflects on the composite score as required by the risk analysis model. To complete the risk analysis, these could be further classified based on priority of implementation of risk mitigation strategies. Priority 1 as area accorded top priority for controls implementation, which would normally require a higher degree of preventative controls and lower priority requiring relatively lesser investments based on the strategy. The risk analysis exercise results in identification of the gaps in controls and the degree of controls, which helps the auditor to plan his efforts accordingly.
- ▶ The risk analysis exercise would also help in identifying the areas of risks and controls which need priority audit attention. Such decisions would also need to cover for example, areas which have undergone detailed audits in the recent past being accorded lower priority and areas that have not undergone an audit being assigned a higher priority.

Exhibit: Sample Information Classification Model

S No.	Application System/ Information Asset	Owner	Criticality			Information Class Rating
			C	I	A	
1	Payroll Processing/ Payroll Data	Manager- Payroll	3	4	4	Internal – Vital
2	Product Research	VP-Product	5	3	3	Internal– Confidential
3	Customer Processing/ Customer Database	VP-Sales	4	4	5	Sensitive - Critical

The following page gives an illustration of a Risk Assessment exercise in the case of email security.

Risk Assessment – E-mail Security**Exhibit: Template for Risk Assessment Observation**

BRIEF DESCRIPTION OF RISK	E-mail suffers from significant risks of unauthorized disclosure, unauthorized modification of mail content or loss of mail in transit due to technical problems either at the server end or the client system end. Mails could contain sensitive information such relating to the customer communications, matters internal to the company etc. Hence the risks of unprotected mail and mail systems pose a critical risk to the organisation: • One of the prime issues in e-mail security is authentication. In an electronic mail system it is difficult to establish, beyond doubt, the authenticity of the sender as well as the mail content. Hence if based on the information in mail, business decisions are driven, without ensuring authenticity of the mail content or without assuring on the sender's identity, this could present critical business risks. Controls such as digital signature systems should be put in place by the organisation • With regard to confidentiality, the organisation would also need to put in a e-mail security policy that ensures the right access control technology coupled with good user management procedures that require users to follow good security practices such as good passwords, care at the time of forwarding mail etc. • The technology used for e-mail should also ensure timely delivery of messages. It is technically possible that due to the inherent risks of the technology, a message may not reach the addressee at all. In such cases, the sender should be informed of the non-delivery of the message. The date and time stamping of mails is also a critical control. • Other broader issues such as the right technology, perimeter controls such as firewalls, right encryption standards, riding on the Internet backbone and the risks thereof should also be carefully considered as regards the controls.

Module 7, Chapter 3

CRITICALITY	7 of 10
RISK	High
IMPACT	Reputation: Significant impact on reputation, if attack on e-mail systems are known to public and customers. The sensitive nature of the business of the organisation would also have bearing on the criticality rating of the risk. For example where the company is an Internet service provider, failure of e-mail security would impact a significant mass of customers and affect the business of the clients critically. Operational: Critical decisions may result in adverse impact, due to e-mail messages which are either intentionally or unintentionally manipulated. Some of such decisions and their impact may be irreversible e.g. awarding a large contract to a ineligible vendor. Legal and Regulatory: Where communication by e-mail is sent to customers of a bank, the bank may be liable for serious action of the regulators -e.g. bank statements delivered to wrong e-mail addresses. The impact of such actions may be significant based on the statutes and regulations in force e.g. the Information Technology Act imposes severe stipulations on what constitutes “delivery of offer”, “acceptance” etc. Efficiency: Inefficient e-mail systems may silently hamper the growth of the organisation itself. Risks such as spamming consume enormous resources both in terms of IT resources as well as management time. Overall Impact Rating: High to Very High
VULNERABILITIES	Depending on the technology and manual controls, the probability of a threat materializing could be significant as they increase the probability of threats materializing. For example, indiscipline amongst users in sharing passwords of critical e-mail accounts may present significant control issues. For example, a bank manager may share his password with his staff. Similarly lack of proper firewall controls, anti-virus controls and unrestricted port services may also result in serious risks. Rating: Moderate to High

Factors for Audit Planning

Scheduling, Assessment of duration, Assessment of skill sets, competence requirements, independence, use of CAATs, project scheduling and management

Audit should be appropriately supervised. This ensures that the audit objectives are achieved and applicable professional auditing standards

and guidelines are complied with. Auditors should obtain sufficient, reliable, relevant and useful evidence for effective audit. Appropriate analysis and interpretation of such evidence should support the audit findings and conclusions.

Based on preliminary evaluation, the auditor should also ascertain the need to obtain the services of an expert. If such an option is exercised, the auditor should ensure compliance with the Auditing and Assurance Standard on “Using the services of an Expert”, while using the services of the expert.

Some of the other factors to be considered at the time Planning for IS Audit include:

a. Changes in fundamental premise

Changes in company management, technology environment, control framework, policies and procedures. The risk rating should consider such entity level controls including changes that may be in progress or planned.

b. Transaction Cycle and Volume

In some cases, processing error rates fluctuate with transaction volume. In such cases the analysis should include a rating for transaction volume. High volume areas are assigned appropriate risk scores depending on the nature of such transactions. The study of transaction cycle e.g. a internet bank transaction could span various systems across various locations and systems across geographical locations and could be completed without any manual intervention. This would be critical in enabling the auditor to plan for the significant use of computer assisted audit techniques and generalized audit software.

c. Frequency

The volume, transaction cycle time and frequency of transactions would have significant impact on the evaluation of the controls e.g. in the case of a stock broking business, the controls should be highly automated. The traditional manual methods of historic or even concurrent review of transactions, whether by the management of internal auditors would be totally ineffective. This requires the examination of the application software for necessary internal controls to protect against significant risks both in terms of business risks (such as unconfirmed click by a user leading to a buy instead of a sell) as well as technology risks such as viruses and hackers.

This would also require consideration on the frequency of audits of the area itself. Some areas would not only require concurrent auditing techniques but also more frequent periodic review by internal/information systems auditors.

d. Value and Materiality

The risk rating score varies with the rupee effect that a given area has on the financial, operations, legal and compliance issues and reputation of the organisation. Monetary loss could result either directly (e.g. loss of control over inventory due to poor application controls) or indirectly (e.g. loss of customer database to competitor). The ratings would need to consider the monetary value of the items processed.

Audit of Outsourced Activities

In case of audit of outsourced activities, the IS auditor should review the criticality of dependence of the client enterprise with respect to the activities or processes outsourced to the external service provider. The IS auditor should also review the service level agreement with the service provider and study the previous audit reports.

Materiality

An important task of the planning phase is the agreement on and establishing levels of materiality. The establishment of materiality threshold is important to ensure the effective utilization of the audit effort. The materiality thresholds should be so fixed such that they do not adversely impact on the effectiveness of the audit and yet enable achieving efficiency. For example, while reviewing the systems for audit, the auditor may choose to not include application software that may not have significant impact in terms of the transaction value and criticality.

The important difference between financial audit and Information systems audit to be noted is that while in the case of the former, the tests are based on monetary measurement, however in the case of Information Systems audits, the impacts as relating to materiality may not always be easily measurable in monetary terms hence it must be understood that establishing materiality thresholds in case of Information Systems audits involves not only quantitative but also should consider qualitative factors e.g. unstructured code design, screen designs which are not mapped to source documents, physical security controls etc. There may be several non-compliance issues such as improper setting in firewalls that present with potential risks. Hence such issues involve significant experience and professional judgment in assessing the composite impact of various apparently significant and insignificant errors and deviations. Fixation of materiality thresholds may also involve establishing thresholds for each category of controls, which are not normally found in financial audits.

After the completion of audit, the impact of individual audit findings as well as the composite impact of individual findings combined with each other should also be evaluated independently to determine their relevance for reporting.

Evidence Collection and Evaluation

The deliverable or the end product of the Information Systems Audit, like most other audits is the audit report. But the raw material for the audit report is the audit evidence, based on which the auditor forms his audit judgement. Audit Evidence includes all the information on which the auditor relies on arrive at his audit opinion. In an Information Systems Audit such information would include significant parts of information that are in electronic form.

Examples of evidence used in Information Systems audit include:

- ▶ logs relating to transactions, systems events or accounting logs generated by application software, database management systems, systems software etc.
- ▶ results obtained by the use of CAATs e.g. the results obtained from a generalized audit software or data extraction and analysis tools
- ▶ electronic files containing system information on parameter settings
- ▶ program listings, control documents such as Batch job control sheet
- ▶ systems development and testing documentation

Besides the above, information obtained from conventional audit procedures may also be important such as:

- ▶ observations – e.g. Inspection of physical controls, employee practices
- ▶ physical and electronic examination of media such as tapes, CDs etc.
- ▶ written policies, procedures and guidelines
- ▶ benchmarking reports, Product information and testing reports
- ▶ systems Flowcharts, Data Flow diagrams, Control Charts
- ▶ information obtained during interview with management and personnel

Such evidence can be obtained by application of audit procedures or a combination of:

- ▶ inquiry and Interviews with management as well as users
- ▶ observation of processes
- ▶ inspection of electronic as well as non-electronic records and processes
- ▶ confirmation of findings through representation of information by external or independent or objective source
- ▶ recalculation, Re-performance and Use of analytical procedures

The information obtained could broadly be categorised as:

- ▶ auditor's recording based on observation of processes
- ▶ audit Evidence in form of documents or in electronic forms

Module 7, Chapter 3

- ▶ management Representations and declarations such as policies and procedures and minutes of Audit committee, Steering committee meetings etc.
- ▶ results obtained by the auditor from application of analytical procedures

An important issue with the evidence in electronic form is that, in the absence of controls, such evidence is subject to tampering without trace of such tampering. For example direct manipulation of values in a database may not be detected unless preventive and detective controls are put in place. Hence one of the important qualities of the evidence that the auditor should ensure at the time of such collection is to secure the time and source of such evidence in such a manner that such evidence is capable of being retrospectively retrieved and verified.

The principles laid out in the Auditing and Assurance Standard on “Basic Principles Governing and Audit” can be extended to Information Systems Audits as well:

- ▶ The Auditor should obtain sufficient appropriate audit evidence through the performance of compliance and substantive procedures to enable him to draw reasonable conclusions therefrom on which to base his opinion on the information resources audited.
- ▶ Compliance procedures are tests designed to obtain a reasonable assurance that those internal controls on which audit reliance is to be placed are in effect. The auditor should obtain sufficient evidence to support his reliance on such controls designed and put in place by the management.
- ▶ Substantive procedures are designed to obtain evidence as to the completeness, accuracy, and validity of the adequacy of the existing internal and IT controls.
- ▶ Such substantive procedures focus on broadly two types:
 - ▼ Tests of details of transactions and balance. Where financial values are involved, the controls in application software and the integrated controls could be put to test. In case of Information Systems audit, not involving financial values, such tests, where financial values may not be applicable could evaluation of efficacy of control e.g. While the evaluation of compliance with change management guidelines may find all guidelines are complied with an intrinsic evaluation of some change requests, independent of the change management guidelines may reveal that the changes do not require a express sign off of the users, which may raise questions on the efficacy of the guidelines itself.
 - ▼ Analysis of significant ratios and trends including the resulting enquiry of unusual fluctuations and items in exceptions. Such tests on financial and as well as non-financial parameters are

useful in determining deviations and exceptions that help identify weak controls or inadequacy in controls.

Types of audit evidence

During the planning for IS audit work, the IS auditor should consider the quality of evidence required with respect to various audit objectives. The nature and degree of audit procedures would be significantly impacted by the quality of evidence desired.

- ▶ Audit objectives required to be achieved in consideration of the nature of business e.g. audit of a departmental store against a stock broking business
- ▶ Independence and relationship of the provider of the evidence to the organisation/area being audited
- ▶ The objectivity and source of evidence – Evidence obtained should be such that it is independently verifiable and capable of being obtained by any person. The source of evidence would also affect the quality of the evidence.
- ▶ Oral evidence can also provide the auditor with significant insights into certain risks but unless documentary assertion or declaration is also obtained to the effect, the same may not be useful unless the auditor uses additional audit procedures to obtain evidence to substantiate the submissions.

Audit Program, Audit procedures and Audit techniques

Like any other audit, Information Systems audit should also follow a structured approach. This is especially so since improper assessment of nature and extent of audit work may lead to an ineffective audit and wasted audit resources.

The ISA 500 on “Planning” also requires the auditor should develop and document an audit program setting out the nature, timing and extent of planned audit procedures required to implement the overall audit plan. The audit program serves as a set of instructions to assistants involved in the audit and as a means to control and record the proper execution of the work. The audit program may also contain the audit objectives for each area and a time budget in which hours are budgeted for the various audit areas or procedures.

In preparing the audit program, the auditor would consider the specific assessments of inherent and control risks and the required level of assurance to be provided by substantive procedures. The auditor would also consider the timing of tests of controls and substantive procedures, the coordination of any assistance expected from the entity, the availability of assistants and the involvement of other auditors or experts.

Hence an audit program is an essential documented control to enable smooth, sequential completion of audit activities and enables assessing

the progress of audit at any point of time. It is also quite possible that the audit program may itself require changes depending on newer information and trends coming to light as the audit progresses. For example, the audit may restricted testing of backups based on results obtained at the time of compliance testing but a substantive test on a sample item such as say, payroll backup may show a corrupted media, indicating the lack of efficacy of recovery testing. This may necessitate the auditor to extend the recovery testing to cover all critical datasets, thus resulting in need for extended audit schedule and resources. The auditor may also be faced with situation wherein the extended audit may be necessary but not justified by the enormous audit resources or extended schedule required. In such a situation, the auditor may be faced with the necessity of qualifying his opinion or even a disclaimer.

Developing an Audit Program

The Audit program should take into consideration the information obtained by the auditor as part of his preliminary review and be so designed to enable effectively achieving the audit objectives and support the audit plan. The principles laid out in the Auditing and Assurance Standard on “Audit Planning” as regards audit program would also apply while drawing up an audit program for information systems audits:

- ▶ The auditor should prepare a written audit program setting forth the procedures that are needed to implement the audit plan. The program may also contain the audit objectives for each area and should have sufficient details to serve as a set of instructions to the audit team members, involved in the audit and as a means to control the proper execution of the audit work.
- ▶ In preparing the audit program, the auditor, having an understanding of the information systems and related business, internal and technology controls, may wish to rely on certain of these controls in determining the nature, timing and extent of required auditing procedures. The auditor may conclude that relying on certain internal controls is an effective and efficient way to conduct his audit. However the auditor may also decide not to rely on internal controls when there are other more efficient ways of obtaining sufficient appropriate audit evidence (e.g. by application of CAATs). The auditor should also consider the timing of the procedures, the co-ordination of any assistance expected from the client, the availability of audit resources and the involvement of other auditors or experts.
- ▶ The auditor normally has flexibility in deciding when to perform audit procedures. However in some cases, the auditor may have no discretion as to timing, for example when observing controls during data migration, testing during implementation etc.
- ▶ The audit planning ideally commences at the conclusion of the previous year or period's audit and along with the related programme,

it should be reconsidered for modification as the audit progresses. Such consideration is based on the auditor's review of the internal controls, his preliminary evaluation thereof, and the results of his compliance and substantive procedures audit.

- ▶ IS audit requires audit programmes to be prepared, taking into consideration the technology environment and the related business process controls. Techniques such as use of Internal Control Questionnaires (ICQs), checklists are extremely useful in the audit of technology controls as well as audit of general controls. Such questionnaires should be appropriately designed so as to achieve the audit objective. The ICQ design should collect information about the business area, data and process flow, and related controls so as to help the auditor in identifying the key controls and risk areas. Standard ICQs can also be developed based on certain standard technology, which can be applied with minimal or no modifications e.g. auditing Windows Server Security. However care should be taken by the auditor to include special considerations that may have come to his knowledge as part of the preliminary evaluation.

Internal Control Questionnaires offer advantages in enabling effective audit planning, implementation as well as during preliminary review phases. An ICQ evolves over time with modifications based on learning in various audits and results in an effective tool to provide significant advantages in terms of efficient utilization of audit resources, timing of audit resource usage and standardization of audit procedures. However there is a tendency to adopt internal control questionnaires and checklists without any modification that may be critically required and exclusive to the audit environment or audit subject area. Such an approach should be avoided since the same could impact on the audit risk.

Use of Sampling in Information Systems Audits

Sampling is used when time and cost considerations preclude a 100 percent verification of all transactions and events in a predefined population. The population consists of the entire group of items that needs to be examined. The subset of population members is called a sample. Sampling is used to infer characteristics of a population, based on the results of examining the characteristics of a sample of the population.

In case of information systems audit, the knowledge of CAATs can have significant impact on the auditor's work. Using CAATs, it may be quite possible to examine 100% of the population instead of samples however it should also be understood that in case of Information Systems audit, other considerations come into play. For example in case of banks using core banking solutions, the entire transaction database of the bank could be centralized. In such case, the entire audit function would be achieved by a small IS audit team using CAATs with capabilities of re-

Module 7, Chapter 3

mote audit of transaction controls. In such an environment the auditors do not have much transaction audit work at the branches since the computers at the branches are mere nodes connecting to the central database. Using CAATs may also adversely impact on the operational efficiency of the business operations since CAATs could consume enormous IT resources. These are some of the reasons that the audit would need to consider sampling in IS audits.

The Auditing and Assurance Standard (AAS 15) “Audit Sampling” provides the related standards on the design and selection of an audit sample and the evaluation of the sample results. This AAS applies equally to both statistical and non-statistical sampling methods. Either method, when properly applied, can provide sufficient appropriate audit evidence.

The IS Auditor should consider selection techniques which result in a statistically based representative sample for performing compliance or substantive testing. Four sampling methods are commonly used:

Statistical Sampling Methods

Random sampling – Ensures that all combinations of sampling units in the population have equal chances of selection.

Systematic sampling: Involves selecting sampling units using a fixed interval between selections. The first interval has a random start. Examples include Monetary Unit Sampling or Value weighted selection where each individual monetary value (e.g. Rs.1) in the population is given an equal chance of selection. As the individual monetary unit cannot be ordinarily be examined separately, the item, which includes the monetary unit is selected for examination. . Another example includes selecting every nth sampling unit.

Non-Statistical Sampling Methods

Haphazard sampling: The IS Auditor selects the sample without following a structured technique, but avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population.

Judgmental Sampling: The IS Auditor places a bias on the sample (e.g. All sampling units over a certain value, all for a specific type of exception, all negatives, all new users, etc.). A judgmental sample is not representative of the population and is not statistically based so the results should not be extrapolated over the population.

The IS Auditor should select sample items such that it is representative of the population. The selected sample should represent all the characteristics of the population being tested. This is done by statistical sam-

pling methods. In order to maintain audit independence, the IS Auditor should ensure the population is complete and control the selection of the sample.

For a sample to be representative of the population, all sampling units in the population should have an equal or known probability of being selected i.e. statistical sampling methods should be used. There are two commonly used selection methods: selection on records, and selection on quantitative fields (e.g. monetary units)

Methods in Use (For selection on records):

- ▶ Random Sample (Statistical sample)
- ▶ Haphazard Sample (Non statistical)
- ▶ Judgmental Sample (Non statistical: high probability to lead to a biased conclusion)

Examples of compliance testing of controls where sampling could be considered include user access rights and authorizations granted, program change control procedures, documentation, follow up on exceptions, review of logs, software license audits etc.

Examples of substantive tests where sampling could be considered include re-performance of complex calculation (e.g. Interest) on a sample of accounts, sample of transactions to vouch to supporting documentation etc.

When using sampling methods either statistical or non-statistical, the IS Auditor should design and select an audit sample, perform audit procedures and evaluate the sample results. Thus he can obtain sufficient, reliable, relevant and useful audit evidence. In forming an audit opinion, IS Auditors generally do not examine all of the information available. This is because it may be impracticable and valid conclusions cannot be reached using audit sampling.

Audit sampling is defined as the application of audit procedures to less than 100% of the population. IT enables the IS Auditor to evaluate audit evidence about some characteristic of the items selected to form or assist in forming a conclusion concerning the population.

Statistical sampling uses techniques from which mathematically constructed conclusions regarding the population can be drawn. Non-statistical sampling is not statistically based and the results should not be extrapolated over the population, as they may not be representative of the population. When designing the size and structure of an audit sample, IS auditors should consider the specific audit objectives, the nature of the population, the sampling and the selection methods. The IS auditor should also consider the need to involve appropriate specialists in the design and analysis of samples.

Sampling Unit

The sampling unit depends on the purpose of the sample. For compliance testing of controls, attribute sampling is typically used, where the sampling unit is an event or transaction (e.g. A control such as “to determine invoices that are not duly authorized”)

For substantive testing, on the other hand, variable or estimation sampling is frequently used and the sampling unit is often monetary. (e.g. Testing of inventory, debtors etc.)

Audit objectives

The IS auditor should consider the specific audit objectives to be achieved and the audit procedures which are most likely to achieve those objectives. In addition, when audit sampling is appropriate, he should consider the nature of the audit evidence sought and possible error conditions.

Population

The population is the entire set of data from which the auditor wishes to sample in order to reach a conclusion on the population. Therefore, the population from which the sample is drawn should be appropriate and verified. Also it must be complete for the specific audit objective.

Stratification

Stratification may be necessary for designing the sample efficiently and effectively. Stratification is a process of dividing a population into sub-populations (strata) with similar characteristics explicitly defined so that each sampling unit can belong to only one stratum.

Sample size

When determining sample size, the IS auditor should consider the sampling risk, the amount of the error that would be acceptable and the extent to which errors are expected.

Sampling risk

Sampling risk arises from the possibility that the IS auditor’s conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risks:

The risk of incorrect acceptance: The risk that material mis-statement is assessed as unlikely when in fact the population is materially mis-stated.

The risk of incorrect rejection – The risk that material mis-statement is assessed as likely when actually the population is not materially mis-stated.

The level of sampling risk that the IS auditor is willing to accept affects the sample size.

Sampling risk should also be considered in relation to the audit risk model and its components, inherent risks, control risks and detection risks.

Tolerable error

Tolerable error is the maximum error in the population that IS auditors are willing to accept and still conclude that the audit objectives have been achieved. For substantive tests, tolerable error is related to the auditor's judgment about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the IS auditor is willing to accept.

Expected error

If the IS auditor expects errors in the population, he selects a larger sample than when no error is expected. This helps to conclude that the actual error in the population is not greater than the planned tolerable error. Similarly, lower sample sizes are justified when the population is expected to be error free. When determining the expected error in a population, the auditor should consider such matters as error levels identified in previous audits, changes in the organisation's procedures and evidence available from an evaluation of the system of internal control and results from analytical review procedures.

The audit work papers should include sufficient details to clearly describe the sample objective and the sampling process used. The work papers should include the source of the population, the sampling method used, sampling parameters (e.g. random start number or method by which random start was obtained, sampling interval), items selected, details of audit tests performed and conclusions reached.

Having performed appropriate audit procedures on each sample item, he should analyse any possible errors detected in the sample. He can thereby determine whether there are actually errors and their nature and cause and the possible effect of the error on the other phases of the audit. He should consider the qualitative aspects of the errors. The errors should be projected as appropriate to the population, if the sampling method used is statistically based.

Errors caused by breakdown of an automated process ordinarily have wider implications for error rates than human errors. When the expected audit evidence regarding a specific sample item cannot be obtained, the auditor may be able to obtain sufficient and appropriate audit evidence by performing alternative procedures on the item selected.

Module 7, Chapter 3

The IS auditor should consider projecting the results of the sample to the population with a method of projection consistent with the method used to select the sampling unit. The projection of the sample may involve estimating probable errors and estimating any undetected errors due to imprecision of the technique together with the qualitative aspects of any errors found.

The IS auditor should consider whether the errors in the population might exceed the tolerance error. While doing so the results of the other audit procedures relevant to the audit objective must be taken into account. If the projected population error exceeds the tolerable error, the IS auditor should reassess the sampling risk. If the risk is unacceptable he should consider extending the audit procedure or performing alternative audit procedures.

Key steps to construction and selecting samples for an audit test:

- ▶ Determine the objectives of the test (e.g. compliance or substantive)
- ▶ Define the population to be sampled
- ▶ Determine the appropriate sampling method, such as attribute vs. variable sampling
- ▶ Determine the precision, reliability and tolerance desired
- ▶ Calculate the sample size
- ▶ Select the sample
- ▶ Evaluate the sample from an audit perspective

Design of the Sample

ISA 530 on “Audit Sampling and other selective testing procedures” prescribes guidelines for designing an audit sample:

When designing an audit sample, the auditor should consider the objectives of the test and the attributes of the population from which the sample will be drawn.

- ▶ The auditor first considers the specific objectives to be achieved and the combination of audit procedures which is likely to best achieve those objectives. Consideration of the nature of the audit evidence sought and possible error conditions or other characteristics relating to that audit evidence will assist the auditor in defining what constitutes an error and what population to use for sampling.
- ▶ The auditor considers what conditions constitute an error by reference to the objectives of the test. A clear understanding of what constitutes an error is important to ensure that all, and only those, conditions that are relevant to the test objectives are included in the projection of errors. For example, in a substantive procedure relating to the existence of accounts receivable, such as confirmation, payments made by the customer before the confirmation date but received shortly after that date by the client are not considered an error. Also, a mis-posting between customer accounts does not affect

the total accounts receivable balance. Therefore, it is not appropriate to consider this an error in evaluating the sample results of this particular procedure, even though it may have an important effect on other areas of the audit, such as the assessment of the likelihood of fraud or the adequacy of the allowance for doubtful accounts.

When performing tests of control, the auditor generally makes a preliminary assessment of the rate of error the auditor expects to find in the population to be tested and the level of control risk. This assessment is based on the auditor's prior knowledge or the examination of a small number of items from the population. Similarly, for substantive tests, the auditor generally makes a preliminary assessment of the amount of error in the population. These preliminary assessments are useful for designing an audit sample and in determining sample size. For example, if the expected rate of error is unacceptably high, tests of control will normally not be performed.

However, when performing substantive procedures, if the expected amount of error is high, 100% examination or the use of a large sample size may be appropriate.

Evaluating the Sample Results

The auditor should evaluate the sample results to determine whether the preliminary assessment of the relevant characteristic of the population is confirmed or needs to be revised.

- ▶ In the case of a test of controls, an unexpectedly high sample error rate may lead to an increase in the assessed level of control risk, unless further evidence substantiating the initial assessment is obtained. In the case of a substantive procedure, an unexpectedly high error amount in a sample may cause the auditor to believe that an account balance or class of transactions is materially misstated, in the absence of further evidence that no material misstatement exists.
- ▶ If the total amount of projected error plus anomalous error is less than but close to that which the auditor deems tolerable, the auditor considers the persuasiveness of the sample results in the light of other audit procedures, and may consider it appropriate to obtain additional audit evidence. The total of projected error plus anomalous error is the auditor's best estimate of error in the population. However, sampling results are affected by sampling risk. Thus when the best estimate of error is close to the tolerable error, the auditor recognizes the risk that a different sample would result in a different best estimate that could exceed the tolerable error. Considering the results of other audit procedures helps the auditor to assess this risk, while the risk is reduced if additional audit evidence is obtained.

Module 7, Chapter 3

- ▶ If the evaluation of sample results indicates that the preliminary assessment of the relevant characteristic of the population needs to be revised, the auditor may:
 - ▼ Request management to investigate identified errors and the potential for further errors, and to make any necessary adjustments; and/or
 - ▼ Modify planned audit procedures. For example, in the case of a test of control, the auditor might extend the sample size, test an alternative control or modify related substantive procedures; and/or
 - ▼ Consider the effect on the audit report.

Documentation Requirements

As in any other audits, documentation of audit work forms a critical task, which the auditor should retain in support of his audit work. Significant amount of information may be generated during the course of the IS auditor's work. The auditor is required to ensure the evidence obtained by him on which he bases his audit opinion is sufficient, reliable, relevant and useful and enables effective achievement of audit objectives.

The audit documentation generally includes:

- ▶ Basic documents relating to the business, technology and control environment
- ▶ Documents relating to laws, regulations and standards applicable
- ▶ Preliminary review and how the audit objectives and scope were evaluated and agreed upon.
- ▶ Documents relating to Risk analysis
- ▶ Audit plan and progress against plan, Audit programmes
- ▶ Audit procedures as applied to the audit
- ▶ Audit findings, observations, inspection reports, management representations, logs, audit trails and other related evidence
- ▶ Interpretation of audit evidence
- ▶ Audit Report issued
- ▶ Auditee's observations and response to findings and recommendations.
- ▶ Reports by third party experts
- ▶ Peer Reviews

The audit working papers :

- ▶ Aid in the planning and performance of the audit
- ▶ Aid in the supervision and review of the audit work
- ▶ Provide evidence of the audit work performed to support the auditor's opinion

To auditor's work must be documented and organized in a standardised fashion for easy reference in future audits and reference by other auditors. These documents should be maintained so that the auditor can

determine whether the steps of the plan have been carried out. For purposes of easy reference, the documents may be organized as follows:

- ▶ Test work papers
- ▶ Permanent work papers
- ▶ Pending files
- ▶ Report files

Test working papers

The testing work papers, either electronic or otherwise are those prepared or obtained as a result of the compliance and substantive testing procedures performed by the auditor, relevant to the audit engagement. Each working paper should follow a naming convention and numbering convention for naming and numbering of the work papers. The files should also contain a brief description of the content. The compliance test files should contain documentation of:

- ▶ Review of the existing internal controls
- ▶ A summary of the tests conducted
- ▶ Documentation of procedures performed and tools, if any used
- ▶ Supporting documentation of detailed tests

Substantive test files require the same elements as compliance test files except for the review of existing internal controls.

Organisation of audit working papers:

Each document must describe the following:

- ▶ Objective – why the work was done?
- ▶ Work done – what was actually done?
- ▶ Finding – What issues arose?
- ▶ Risk – what are the risks associated with the finding, expressed in terms of impact on business
- ▶ Recommended action – what is being recommended
- ▶ Action – what action was agreed with management
- ▶ Each working paper should be supported by evidence of the weaknesses observed

Documentation Controls

Information systems audit documentation is the record of the audit work performed and the audit evidence supporting the IS auditor's findings and conclusions.

- ▶ Each working paper (or work paper) should be:
 - ▼ Dated and manually or digitally signed by the person completing the work
 - ▼ Referenced with a unique number
- ▶ In case of work papers and evidence in electronic format, special care must be taken to ensure their recoverability at any subsequent date with sufficient controls to prove the date of creation and ensure

against any modifications to the content or the state of such documents. This would require the auditor to use necessary technology such as use of appropriate media for storage of electronic evidence and their assured recoverability, use of digital signatures for protecting authenticity of documents, use of encryption techniques to safeguard the confidentiality of such documents.

- ▶ The auditor should also take care to ensure retention of such audit documentation to be retained for sufficient length of period such that it complies with legal, regulatory, professional and organizational requirements.

Reporting

The audit exercise results in the audit report, which is the deliverable or end product of the audit. The audit report, being the culmination of the auditor's work, should highlight all the key findings and recommendations. The design of the audit report would depend on the terms of engagement and audit objectives. The format and structure of the audit report should be taken into consideration at the audit planning stage itself. The audit report normally results in the identification of control weaknesses or areas of concern. The findings need to be analyzed as to their cause and consequence. Considering the prevalent practices and practical feasibility, the auditor should formulate his recommendations. Each of the findings identified should be ranked as per pre-determined criteria. e.g. High, Medium and Low. Such rankings could be based on risk. The rankings can be further prioritised and discussed with the auditee for accuracy. Feedback from the auditee management has to be obtained for both the findings and recommendations before their inclusion in the final report.

Reporting on control weaknesses

The quality of an audit is not measured by the number of findings reported but by the auditor's evaluation of the control system and identification of its weaknesses. Any existing control weaknesses could be detrimental to the quality of the control systems. Hence evaluation of the quality of the control system is the first priority in an IS audit. The evaluation may take two forms:

1. Review and documentation of the system, whereby the system flow, manual and automated flow is documented in flow chart or narrative form. Points at which control can best be affected whether manual or automated are identified and described. Effectiveness of these control points is evaluated. Weak controls could be documented on a "finding form".
2. Compliance and Substantive test procedures are performed on IT processes to evaluate the compliance with and the efficacy of the key controls during the audit period.

Reporting Audit Findings

During the preliminary review and compliance test phases, weaknesses in internal control may have occurred and been isolated. These are documented in the finding form. Documented weaknesses form the basis for the auditor's report to the management. Proper preparation of the report is extremely important. Appropriate members of the management team and audit staff should be assigned the task of preparing the report. Audit findings during the various audit phases are documented on the findings forms. As each transaction in each phase is completed, the auditor who prepared the finding form should write the comments and recommendations for inclusion in the final audit report.

A typical finding form used to identify control weaknesses is given below: The auditor must identify the condition, causes and effect of the internal control weaknesses

Sample - Control weakness – Audit finding form

CONDITION	The accounts payable online system has 7 on-line update transactions, which are not assigned to specific terminals but could be accessed on any terminal located in the accounts department.
CAUSE	When the accounts payable on-line update programs were modified to include all update transactions in a menu screen format, the old transaction codes were not deleted from the system
EFFECT	Access to the critical payables screen on unauthorized terminals could lead to unauthorized viewing or modifications to such data.
RISK RANKING	High
RECOMMENDATION	The payables menu options should be removed from the profiles attached to other login id and terminals with specific access to the payables options only to the specified Login ID and specified terminals only
MANAGEMENT RESPONSE	Online transaction operations are assigned by the access control systems, only to those who need to use them regardless of the terminal they use. However since accounts payable personnel should use the terminals in the accounts payable processing area and the transaction codes have been replaced by the menu functions, IS will be instructed to remove inappropriate access.

A brief explanation of each of the above terms is given below:

CONDITION	This section describes the problem, or more specifically the exposure. Evidence that the condition exists should be documented with the number of errors.

EFFECT	This section is for the description of the extent of impact or loss that has occurred or potential loss. The probability or potential extent of the exposure should be estimated to the extent possible
RISK RANKING	The auditor's ranking of the risk in terms of the intensity of the observation
RECOMMENDATION	This section describes the possible solution to the problem that the auditor, in discussion with the auditee management feels is appropriate. The management looks at this section as the value add from the IS auditing exercise. The recommendation should be practicable and should provide the solution to the problem.
MANAGEMENT RESPONSE	This section describes the auditee management's response to the audit finding and recommendation

It is important that the auditor must discuss the findings with the audit management before raising the issues in the final report.

The audit report should state at a minimum the following:

- ▶ Audit objectives
- ▶ Audit scope
- ▶ Period of coverage
- ▶ Nature and extent of audit work performed
- ▶ Audit Findings
- ▶ Audit conclusions and recommendations
- ▶ Reservations or qualifications that the auditor may have.

The audit report should also addressed to the intended recipients and specifically mention restrictions as to circulation of the report. The report should be in lucid language, objective, complete and relevant.

Salient Features of the IS Audit Reports

There cannot be standard audit report formats that could be generically applied to every audit. However the contents and format of the IS audit report should contain the minimum requirements as per the reporting standards and the information required by the auditee. IS auditors should consider the specific scope and objectives of audit while designing the format and structure of the audit report. Some salient features of an audit report are given below:

Report Content and Form

An IS auditor should provide a report in an appropriate form to the intended recipients upon the completion of the audit work. The report must state the scope, objectives, period of coverage and the nature and extent of the audit work performed. It should also identify the organisation the intended recipients and state restrictions on distribution, if

any. The report must include the findings, conclusions and recommendations and any reservations or qualifications that the auditor has with respect to the audit.

Purpose and Content

A report is a formal means of communicating the objectives of the audit, the auditing standards used, the audit scope, the methodology and the findings, conclusions and recommendations

Intended Recipients

While preparing the report, the auditor should consider the needs of the intended recipients, which may include the auditee, executive management, the board of directors, the audit committee and the statutory or regulatory authorities

Style and content

The style and content of the report should be appropriate to the intended recipients. It could be in writing, oral or other form. A written report should identify the organisation audited and include a title, a signature and the date

A report on other media may include an appropriate form of authentication instead of a written signature. Reports should be objective, clear, concise, constructive and timely.

Statement of objectives

The report should include a statement of the objectives of the audit to identify what the audit intended to accomplish. If any audit objectives stated in the report were not met, this fact should be disclosed in the report.

Scope of audit

The report should include a statement of the audit scope that describes the nature, timing and extent of audit work performed. The statement of scope should identify the functional audit area, the audit period covered and the information systems, applications or processing environments audited

The report should identify circumstances when there has been limitation on the scope of the audit. There is a limitation of scope when the IS auditor's opinion, tests and procedures appropriate for meeting standards could not be completed, or when an auditee imposed restrictions on the audit work.

Restrictions on distribution

The report should identify the auditee and indicate the date of issue of the report. The report should also specify that it is solely for the information and use of the intended parties such as the auditee, board of di-

Module 7, Chapter 3

rectors, management and any intended parties outside the organisation (e.g. a government agency). Restrictions on its distribution if any should be stated.

Significant findings

The report should include all significant audit findings. When a finding required explanation, the IS auditor describe the finding, its cause and its risk. When appropriate, explanations and reference could be included as attachments. The IS Auditor should also identify the organizational, professional and governmental criteria applied.

Conclusion

The auditor's evaluation may be stated where appropriate. The conclusion may be an overall evaluation or multiple evaluations related to specific audit objectives.

Recommendations

The report should express recommendations for corrective action where possible, Recommendations should be linked to specific findings.

Reservations or qualifications

The report should describe any significant reservations or qualifications and the exposure relating to such qualifications should also be mentioned.

Presentation

The report should be logically organized and presented. It should contain sufficient and relevant information to be understood by the intended recipients

Timeliness

The report should be issued in a timely manner to encourage prompt corrective action. When appropriate, the IS auditor should communicate significant findings promptly to concerned persons issuing the report. Prior communication of significant findings should not alter the intent or content of the report.

Subsequent events

Before issuing the final version of the report, the IS auditor should consider establishing any material changes in the organisation or its environment which might affect the reported findings conclusions and recommendations. When such changes are identified, he should alert the recipients about the potential effect of these changes on the reported findings, conclusions and recommendations.

Follow Up

The effectiveness of an Information Systems Audit is realized on if the action points and recommendations committed and agreed to by the auditee management are implemented. Hence an important task of the auditor is to review the previous audit reports and follow up on the corrective actions and recommendations implemented within the time schedules committed by the auditee management. The status of follow up activities should also be included as part of the audit report.

Annexure 1: AAS 29 - Auditing in a Computer Information Systems Environment

The following is the text of the Auditing and Assurance Standard (AAS) 29, “Auditing in a Computer Information Systems Environment” issued by the Council of the Institute of Chartered Accountants of India (Issued in January 2003). This Standard should be read in conjunction with the “Preface to the Statements on Standard Auditing Practices” issued by the Institute.

Introduction

1. The purpose of this Auditing and Assurance Standard (AAS) is to establish standards on procedures to be followed when an audit is conducted in a computer information systems (CIS) environment. For the purposes of this AAS, a CIS environment exists when one or more computer(s) of any type or size is (are) involved in the processing of financial information, including quantitative data, of significance to the audit, whether those computers are operated by the entity or by a third party.
2. The overall objective and scope of an audit does not change in a CIS environment. However, the use of a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity. Accordingly, a CIS environment may affect:
 - a. the procedures followed by the auditor in obtaining a sufficient understanding of the accounting and internal control system.
 - b. the auditor’s evaluation of inherent risk and control risk through which the auditor assesses the audit risk.
 - c. the auditor’s design and performance of tests of control and substantive procedures appropriate to meet the audit objective.
3. The auditor should consider the effect of a CIS environment on the audit. The auditor should evaluate, inter alia, the following factors to determine the effect of CIS environment on the audit:
 - a. the extent to which the CIS environment is used to record, compile and analyse accounting information;

Module 7, Chapter 3

- b. the system of internal control in existence in the entity with regard to:
 - i. flow of authorised, correct and complete data to the processing center;
 - ii. processing, analysis and reporting tasks undertaken in the installation; and
- c. the impact of computer-based accounting system on the audit trail that could otherwise be expected to exist in an entirely manual system.

Skills and Competence

- 4. The auditor should have sufficient knowledge of the computer information systems to plan, direct, supervise, control and review the work performed. The sufficiency of knowledge would depend on the nature and extent of the CIS environment. The auditor should consider whether any specialised CIS skills are needed in the conduct of the audit. Specialised skills may be needed, inter alia, to:
 - ▼ obtain sufficient understanding of the effect of the CIS environment on accounting and internal control systems;
 - ▼ determine the effect of the CIS environment on the assessment of overall audit risk and of risk at the account balance and class of transactions level; and
 - ▼ design and perform appropriate tests of control and substantive procedures.

If specialised skills are needed, the auditor would seek the assistance of an expert possessing such skills, who may either be the auditor's staff or an outside professional. If the use of such a professional is planned, the auditor should, in accordance with AAS 9, "Using the Work of an Expert", obtain sufficient appropriate audit evidence that the work performed by the expert is adequate for the purposes of the audit.

Planning

- 5. In accordance with the Auditing and Assurance Standard (AAS) 6 (Revised), "Risk Assessments and Internal Control", the auditor should obtain an understanding of the accounting and internal control systems sufficient to plan the audit and to determine the nature, timing and extent of the audit procedures. Such an understanding would help the auditor to develop an effective audit approach.
- 6. In planning the portions of the audit which may be affected by the CIS environment, the auditor should obtain an understanding of the significance and complexity of the CIS activities and the availability of the data for use in the audit. This understanding would include such matters as:

- a. the computer information systems infrastructure [hardware, operating system(s), etc., and application software(s) used by the entity, including changes, if any, therein since last audit].
 - b. the significance and complexity of computerised processing in each significant accounting application. Significance relates to materiality of the financial statement assertions affected by the computerised processing. An application may be considered to be complex when, for example:
 - ▲ the volume of transactions is such that users would find it difficult to identify and correct errors in processing.
 - ▲ the computer automatically generates material transactions or entries directly to another application.
 - ▲ the computer performs complicated computations of financial information and/or automatically generates material transactions or entries that cannot be (or are not) validated independently.
 - ▲ transactions are exchanged electronically with other organisations [as in electronic data interchange (EDI) systems] without manual review for propriety or reasonableness.
 - c. determination of the organisational structure of the client's CIS activities and the extent of concentration or distribution of computer processing throughout the entity, particularly, as they may affect segregation of duties.
 - d. determination of the availability of data. Source documents, computer files, and other evidential matter that may be required by the auditor may exist for only a short period or only in machine-readable form. Computer information systems may generate reports that might be useful in performing substantive tests (particularly analytical procedures). The potential for use of computer-assisted audit techniques may permit increased efficiency in the performance of audit procedures, or may enable the auditor to economically apply certain procedures to the entire population of accounts or transactions.
7. When the computer information systems are significant, the auditor should also obtain an understanding of the CIS environment and whether it may influence the assessment of inherent and control risks. The nature of the risks and the internal control characteristics in CIS environments include the following:
- ▼ **Lack of transaction trails:** Some computer information systems are designed so that a complete transaction trail that is useful for audit purposes might exist for only a short period of time or only in computer readable form. Where a complex application system performs a large number of processing steps, there may not be a complete trail. Accordingly, errors embedded in an application's

program logic may be difficult to detect on a timely basis by manual (user) procedures.

- ▼ **Uniform processing of transactions:** Computer processing uniformly processes like transactions with the same processing instructions. Thus, the clerical errors ordinarily associated with manual processing are virtually eliminated. Conversely, programming errors (or other systemic errors in hardware or software) will ordinarily result in all transactions being processed incorrectly.
- ▼ **Lack of segregation of functions:** Many control procedures that would ordinarily be performed by separate individuals in manual systems may become concentrated in a CIS environment. Thus, an individual who has access to computer Programmes, processing or data may be in a position to perform incompatible functions.
- ▼ **Potential for errors and irregularities :** The potential for human error in the development, maintenance and execution of computer information systems may be greater than in manual systems, partially because of the level of detail inherent in these activities. Also, the potential for individuals to gain unauthorised access to data or to alter data without visible evidence may be greater in CIS than in manual systems. In addition, decreased human involvement in handling transactions processed by computer information systems can reduce the potential for observing errors and irregularities. Errors or irregularities occurring during the design or modification of application Programmes or systems software can remain undetected for long periods of time.
- ▼ **Initiation or execution of transactions:** Computer information systems may include the capability to initiate or cause the execution of certain types of transactions, automatically. The authorisation of these transactions or procedures may not be documented in the same way as that in a manual system, and management's authorisation of these transactions may be implicit in its acceptance of the design of the computer information systems and subsequent modification.
- ▼ **Dependence of other controls over computer processing:** Computer processing may produce reports and other output that are used in performing manual control procedures. The effectiveness of these manual control procedures can be dependent on the effectiveness of controls over the completeness and accuracy of computer processing. In turn, the effectiveness and consistent operation of transaction processing controls in computer applications is often dependent on the effectiveness of general computer information systems controls.
- ▼ **Potential for increased management supervision:** Computer information systems can offer management a variety of analytical tools

that may be used to review and supervise the operations of the entity. The availability of these analytical tools, if used, may serve to enhance the entire internal control structure.

- ▼ **Potential for the use of computer-assisted audit techniques:** The case of processing and analysing large quantities of data using computers may require the auditor to apply general or specialised computer audit techniques and tools in the execution of audit tests.

Both the risks and the controls introduced as a result of these characteristics of computer information systems have a potential impact on the auditor's assessment of risk, and the nature, timing and extent of audit procedures.

8. While evaluating the reliability of the accounting and internal control systems, the auditor would consider whether these systems, inter alia:
 - a. ensure that authorised, correct and complete data is made available for processing;
 - b. provide for timely detection and correction of errors;
 - c. ensure that in case of interruption in the working of the CIS environment due to power, mechanical or processing failures, the system restarts without distorting the completion of the entries and records;
 - d. ensure the accuracy and completeness of output;
 - e. provide adequate data security against fire and other calamities, wrong processing, frauds etc.;
 - f. prevent unauthorised amendments to the Programmes; and
 - g. provide for safe custody of source code of application software and data files.

Assessment of Risk

9. The auditor should make an assessment of inherent and control risks for material financial statement assertions, in accordance with AAS 6 (Revised), "Risk Assessments and Internal Control".
10. The inherent risks and control risks in a CIS environment may have both a pervasive effect and an account-specific effect on the likelihood of material misstatements, as follows:
 - ▼ The risks may result from deficiencies in pervasive CIS activities such as program development and maintenance, system software support, operations, physical CIS security, and control over access to special-privilege utility Programmes. These deficiencies would tend to have a pervasive impact on all application systems that are processed on the computer.
 - ▼ The risks may increase the potential for errors or fraudulent activities in specific applications, in specific databases or master files, or in specific processing activities. For example, errors are

Module 7, Chapter 3

not uncommon in systems that perform complex logic or calculations, or that must deal with many different exception conditions. Systems that control cash disbursements or other liquid assets are susceptible to fraudulent actions by users or by CIS personnel.

11. As new CIS technologies emerge for data processing, they are frequently employed by clients to build increasingly complex computer systems that may include micro-to-mainframe links, distributed data bases, end-user processing, and business management systems that feed information directly into the accounting systems. Such systems increase the overall sophistication of computer information systems and the complexity of the specific applications that they affect. As a result, they may increase risk and require further consideration.

Audit Procedures

12. In accordance with AAS 6 (Revised) "Risk Assessments and Internal Control", the auditor should consider the CIS environment in designing audit procedures to reduce audit risk to an acceptably low level. He should make enquiries and particularly satisfy himself whether:
 - a. adequate procedures exist to ensure that the data transmitted is correct and complete; and
 - b. cross-verification of records, reconciliation statements and control systems between primary and subsidiary ledgers do exist and are operative and that accuracy of computer compiled records are not assumed.
13. The auditor's specific audit objectives do not change whether accounting data is processed manually or by computer. However, the methods of applying audit procedures to gather evidence may be influenced by the methods of computer processing. The auditor can use manual audit procedures, or computer-assisted audit techniques, or a combination of both to obtain sufficient evidential matter. However, in some accounting systems that use a computer for processing significant applications, it may be difficult or impossible for the auditor to obtain certain data for inspection, inquiry, or confirmation without computer assistance.

Documentation

14. The auditor should document the audit plan, the nature, timing and extent of audit procedures performed and the conclusions drawn from the evidence obtained. In an audit in CIS environment, some of the audit evidence may be in the electronic form. The auditor should satisfy himself that such evidence is adequately and safely stored and is retrievable in its entirety as and when required.

Effective Date

15. This Auditing and Assurance Standard (AAS) becomes operative for all audits related to accounting periods beginning on or after 1st April, 2003.

Compatibility with International Standard on Auditing (ISA) 401

The auditing standards established in this Auditing and Assurance Standard are generally consistent in all material respects with those set out in International Standard on Auditing (ISA) 401 on Auditing in a Computer Information Systems Environment except for the additional requirement related to “Documentation” [see paragraph 14]. ISA 401 does not contain any requirement related to documentation.

Annexure 2: Sample UNIX Audit Checklist

1. Verify the Root permissions and the justifications for the same.
2. Verify the Groups created and the access rights. For example: O/S accessibility for the System administrator only. Likewise all permissions must justify the organizational positions and policies.
3. Verify logs for all users including the ‘su’ super user
4. Verify all batch jobs initiated during the start up process and the purpose. Verify the user rights and allocation of responsibility etc.
5. Conduct periodic password checks for quality of passwords.
6. Verify use of forced logs offs after period of inactivity.
7. Verify utilities that have been developed for administration of the network, so as to confirm their accessibility.
8. Verify the result of the use of ‘su’ switch user command should be deactivated for all except the sysadmin. (system administrator)
9. Verify the ‘tty’ definitions terminal nos. This could be an effective tool for logging the terminals in a network and also for allocation of rights on a terminal basis.
10. Verify the rights for the allocation of the tty nos. to ensure that the users are not allowed access to set tty nos. which could result in the spoofing of the tty no. by a person with malicious intentions.
11. Verify the restrictions on the use of the Tenet tactility on terminals handling sensitive data.
12. Verify all interfaces between the O/S and the application system or the RDBMS running on it to ensure that access to the O/S is not found as a result of system exits
13. Verify the disability of the grep command so as to ensure that the search facility for the entire system is restricted only to the sysadmin. (In case the login by the user takes him to the user home directory prompt).
14. Verify all corncoobs.
15. Verify whether all users are taken to the application they are allowed to access and that they do not have access to the user home directory prompt in Unix. This will ensure that no one has access to conduct

Module 7, Chapter 3

- any operations on the directory. It will also ensure that there is no accidental or deliberate erasure of files from a given directory.
16. Verify whether the log records the following events both successes and failures:
 - ▼ Login and Logout attempts
 - ▼ Use privileged commands
 - ▼ Use of print commands
 - ▼ Access Control permissions and modification
 - ▼ Transfer of data to media
 - ▼ Unauthorized access attempts
 - ▼ System startup and shutdown.
 17. In case there are situations that require the allocation of such permissions, examine justifications for the same.
 18. Does the above log contain the following details?
 - ▼ Date and time of the event
 - ▼ User ID
 - ▼ Type of event
 - ▼ Success or failure of the transaction
 - ▼ Origin of the request - tty no.
 19. As Unix is extremely sensitive to disruption in power, verify whether the computer system has uninterrupted power supply to the Unix server so that the system does not crash.
 20. Verify whether the start up and shutdown process of the Unix operation system are conducted in systematic manner to ensure that all processes are properly commenced and terminated.

Annexure 3: Sample IS Audit Finding - Logical Access Controls Review of Operating System

We have reviewed procedure of granting access to the Operating System (OS). Our specific findings and recommendations with agreed action plan are given below: The overall control objective in implementing OS Access Controls:

“The creation of users and their access need to be controlled through appropriate authorization levels. Controls have to be laid down and adhered to while granting authorization. Access logs are to be generated whenever the O/S is accessed and Access logs should show details as to the users accessing the O/S , the period of access and the resources accessed . System must enforce a systematic procedure for logins and logouts. All access points to the system are to be monitored by way to access logs and these access points are available only on the administrators console and terminals”.

1 System Users have blank user ID:

ISSUE:

Presently, the system manager has the system administration rights and toll manager is also created as a user who can modify the ini (initial) settings in PQR. These users have a blank users ID and passwords have not been changed since installation.

IMPLICATIONS: High

User accountability may not be established on account of lack of documentation. 'The operations of PQR may be affected in case of breakdown and non-availability of the relevant personnel.

RECOMMENDATIONS:

- ▶ The users of Operating System and Toll operations Package in PQR Computer need to be authorized in writing by senior management. Creation of their user id and password should be documented and accepted by the user and kept by senior management in sealed cover in safe custody to be available in case of need.
- ▶ Password policy has to be formulated and passwords should be changed at least once in 90 days without being reused.

XYZ LTD'S COMMENTS:

Agreed. System manager will create user ids for all authorized users.

2. PQR Computer is networked to Other Computers

ISSUE:

The PQR Computer is linked to other Computers in the Network. These computers are only being used by the Toll staff for performing jobs such as preparing Toll Reports. Networking of these office computers with PQR computer makes it vulnerable to unauthorized access.

IMPLICATION: High

PQR System could be accessed by any of the users of the office computers.

RECOMMENDATIONS:

A review of security and operations settings needs to be done and all access to PQR Computer from any of the office computers has to be removed or restricted.

XYZ LTD'S COMMENTS:

Agreed. Will be reviewed and modified as required.

Annexure 4: Sample IS Audit Report (Extract)

Objective of the assignment

The primary objective of this information Systems Audit assignment was to provide assurance to the management of ABC Limited (ABC) on the availability, appropriateness and adequacy of controls in the Financial Accounting and Loan Processing System (FALPS) through review of the

Module 7, Chapter 3

control framework of their in-house package- Financial Accounting and Loan Processing System (FALPS), review of Logical access controls of FALPS and conduct Implementation audit of General Controls at 2 select branches.

Proposed scope of review / Terms of reference

Based on the understanding of ABC's needs for conducting systems audit of FALPS package, it was decided to primarily focus on review of data integrity in FALPS package. The review of FALPS package aimed to provide comfort on the adequacy and appropriateness of controls and data so as to mitigate the following system operational risks and ensure that the information systems are implemented so as to provide a safe and secure computing environment. The detailed scope of review/methodology was also agreed upon. Broadly, the overall scope of review primarily from security/controls involved the following: Application controls at various stages such as Input, Processing, output, Storage, Retrieval and Transmission so as to ensure Confidentiality, Integrity and Availability of data. Further, organisational structure policies, procedures and practices as mapped in the information systems focusing on efficiency/controls were also reviewed.

The following areas were reviewed:

Logical Access Controls as implemented through:

- a. Operating System Software (Unix) - Access controls
- b. Telecommunications software - Access controls
- c. RDBMS (Oracle) - Access controls
- d. FALPS package - Major focus area - Access, security and effectiveness
- e. Review of General controls at 2 select branches covering environmental and physical access controls review, logical access controls review as implemented, application controls as implemented and review of policies, procedures and practices relation to IT implementation.

Our approach / methodology

The audit was carried out as pre-planned audit plan and program, which was discussed with the statutory auditors and ABC's senior management, The key tasks of our audit plan are highlighted below:

- ▶ Discussions with the IT department and user management.
- ▶ Review of circulars issued by ABC Ltd relating to IT operations
- ▶ Review of Environmental Access and Physical Access controls
- ▶ Review of Operating systems (Unix) and RDBMS (oracle) Manuals
- ▶ Examination of OS and RDBMS access rights
- ▶ Review of FALPS package Technical and user manuals
- ▶ Examination of access profiles and parameter settings in FALPS package

- ▶ Review of application controls in FALPS package
- ▶ Observation of the users and the system in operation
- ▶ Examination of processing controls in FALPS using test data
- ▶ Review of Reports and Audit Logs in System Software and FALPS package

Audit environment

We conducted IS audit at the IT department of ABC in a simulated environment using a Windows NT Terminal connected to Pentium Server with SCO UNIX as Operating System and RDBMS as Oracle using latest version of FALPS with copy of data of Bangalore Branch (up to 31st march 2002). We have also visited reviewed two branch operations.

Audit reports

We issued a draft report outlining our issues and recommendations and have obtained feedback from the IT Department. Further, a meeting was held with IT department represented by Mr.Sam, AGM (IT) and Mr.Ram, AGM(Finance and Accounts) where the issues and recommendations were discussed in detail. The IT Department has been very proactive in incorporating our suggestions. The issues rectified so far are given separately in Annexure-3 for the purpose of record. The report incorporates all the issues, which have been agreed upon and confirmed. This IS audit report includes the following annexure and has to be read in its totality:

1. Summary of Findings: Outlines all key issues with exposures
2. Specific Issues and recommendations: Issues which need to be implemented
3. Issues identified which have been rectified by it dept. Issues rectified as on date
4. Logical access control Review of Unix: Access Controls issues of Unix.
5. Logical access control Review of Oracle: Access Controls issues of oracles.
6. Review of data using SQL: Highlights data integrity issues in existing data

Overall Conclusions

Based on the review our overall conclusions on specific areas are:

a. Security and access controls

Our review of security and access controls at the IT Environment as reviewed by us and as implemented in ABC using Unix, Oracle and FALPS confirms that appropriate security and access controls have been implemented by using related functions and features of the packages. Our test checks revealed that the systems of security and controls are reliable. However, controls in certain areas need to be strengthened Vide Annexure.

Module 7, Chapter 3

b. Business process controls

Our review of business process validations and data integrity controls covering all the core functions of ABC as facilitated by FALPS such as interest computation, allocation and aging, confirms that all related data has been duly captured, processed and stored correctly and completely, subject to some transaction data not available pertaining to previous years. However, there are also missing data in master tables, which affect the MIS and statements of accounts. The issues identified by us during our review are highlighted in the annexure.

Further action

We consider that the recommendations given in annexure to this report would be very useful for facilitating business process controls of ABC and will aid in improving the effectiveness of FALPS package and computer operations.

We would like to affirm that the matters included in this report are those which came to our notice during our review by following normal information System audit procedures by complying with globally applicable auditing standards, guidelines and procedures that apply specifically to information systems Auditing. Further, on account of limitations of scope and time, we have used sample test and test check approach. Hence, certain areas, which were outside the scope of this review such as source code review, implementation controls and general controls specific to the branches were not covered in the review.

Summary

The chapter discusses in fine detail the process of IS audit: the different phases have been described and the activities therein are detailed. The audit procedures and techniques are explained.

The tech-savvy auditors can use a computer program for audit purpose.

The chapter discusses the documentation associated with audit and report formats.

The auditing standard has been explain and checklists have been shown for sample audits.



4 IS Audit Techniques & Computer Assisted Audit Techniques

✂ Learning Goals ✂

To gain knowledge on various audit methods and techniques available and the factors underlying their selection for auditing in a computerized information system environment, while being aware of the advantages and disadvantages of using CAATs.

Key Objectives

- ▶ Gain a good understanding the IT controls and security and impact of IT environment in selecting the appropriate audit methodology.
- ▶ Gain knowledge on the various methods, techniques and types of tools for auditing in a computerized environment and for IT audits.
- ▶ Understanding of auditing in continuous audit environments.

IT Environment Impact on Audit Methodology

As explained elsewhere in this material, the impact on auditing can be understood to be broadly twofold:

- A. The traditional audit techniques either almost invariably will fail to achieve the traditional audit objectives whether it be external financial audits or internal audits or the cost of audits and the time required would be unjustifiably higher. This can be also referred to as Auditing in a computerized environment
- b. The emergence of newer risks due to introduction of information technology and the very inherent nature of risks that IT suffers from, has also introduced the need for assurance on related security and controls. This can be referred to as conducting an IT Audits.

While the former is more oriented towards testing the transactions, the latter is more oriented towards controls over the Information Technology and IT environment.

Depending on the audit objective, the auditor would have to carefully ascertain the audit methodology and the tools and techniques that would enable the effective and efficient achievement of the audit objectives.

Auditing in a Computerized Information Systems Environment

Information technology has impacted the very manner in which auditing objectiveness is achieved in a computerized environment.. In a Computerized Information Systems Environment (CIS), there is significant impact on financial information and the related systems. The manner in which the internal controls affect the financial and related information will vary significantly and it is required of the auditor to gain a good understanding of the manner and the effectiveness with which the controls are applied in such an environment.

Audit test procedures should be so designed as to be effective and at the same time efficient to ensure a timely and cost-effective audit. It is important for the audit function entrusted with such an objective to take into consideration the Auditing and Assurance Standard 29 on “Auditing in a computerized Information Systems Environment, issued by the council of the Institute of the Chartered Accountants of India.

In this regard, the AAS 29 states:

“The overall objective and scope of an audit does not change in a CIS environment. However, the use of a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity. Accordingly, a CIS environment may affect:

- ▶ the procedures followed by the auditor in obtaining a sufficient understanding of the accounting and internal control system.
- ▶ the auditor’s evaluation of inherent risk and control risk through which the auditor assesses the audit risk.
- ▶ the auditor’s design and performance of tests of control and substantive procedures appropriate to meet the audit objective.

For the purposes of this AAS, a CIS environment exists when one or more computer(s) of any type or size is (are) involved in the processing of financial information, including quantitative data, of significance to the audit, whether those computers are operated by the entity or by a third party.

The AAS 29 specifically requires the auditor to consider the effect of a CIS environment on the audit and requires that:

“The auditor should evaluate, inter alia, the following factors to determine the effect of CIS environment on the audit:

- a. the extent to which the CIS environment is used to record, compile and analyse accounting information;
- b. the system of internal control in existence in the entity with regard to:

- i. flow of authorised, correct and complete data to the processing center;
- ii. processing, analysis and reporting tasks undertaken in the installation; and
- c. the impact of computer-based accounting system on the audit trail that could otherwise be expected to exist in an entirely manual system. “

Audit of IT Controls and Security

The IT environment also presents with a new set of risks that directly or indirectly impact the business risks. Information Technology suffers from inherent risks that can critically impact the business processes and activities in a significant manner. These risks could result from the lack of various controls that include:

- ▶ Lack of an IS Security Policy Framework, procedures and controls
- ▶ Approach for Control over IT and related resources
- ▶ Risks of outsourcing of IT processes
- ▶ Physical and Environmental Security of IT equipments and related assets
- ▶ Poor controls over Communication and Networking technology and infrastructure
- ▶ Poor controls over systems parameter settings and critical systems files
- ▶ Risks from viruses, hackers and malicious code
- ▶ Poor Access Controls over network access, operating systems access, Application access, monitoring
- ▶ Poor Controls over Software Development Life Cycle
- ▶ Poor Business Continuity Planning

Performing IT audits requires a significantly higher level of knowledge of Information Technology and related controls. More importantly, the auditor should be in a position to appreciate the technology risks and controls with regards to the existing and emerging technologies and the related impacts on the business controls. Performing such audits would require the auditor to use various techniques including both traditional audit procedures such as inquiry and observation and sophisticated IT tools to achieve his audit procedures. The use of tools in such audits needs significant care by the auditor to assure and ensure against any possibilities of any integrity risks to the client's environment.

Technical audits such as network penetration testing would involve in-depth knowledge of networking technologies, methods of attack and knowledge of tools that are safe and that can be used for achieving the testing objectives. The auditor should also be knowledgeable of the protocols to be followed in such cases before commencing the testing and after completion of testing.

Skills and Competence

AAS 29 also stipulates the skills and competence requirements as regards auditing in a CIS environment:

“16. The auditor should have sufficient knowledge of the computer information systems to plan, direct, supervise, control and review the work performed. The sufficiency of knowledge would depend on the nature and extent of the CIS environment. The auditor should consider whether any specialised CIS skills are needed in the conduct of the audit. Specialised skills may be needed, inter alia, to:

- ▲ obtain sufficient understanding of the effect of the CIS environment on accounting and internal control systems;
- ▲ determine the effect of the CIS environment on the assessment of overall audit risk and of risk at the account balance and class of transactions level; an design and perform appropriate tests of control and substantive procedures.”

The objective and scope of audit differs with the type of audit i.e. tax audit, statutory audit, internal audit, operational audit etc. Thus, the methodology of audit may vary depending on extent of automation of the audit subject area and related information, and the IT environment at the client's place.

The deployment of IT resources for a specific environment consists of different information technology resources such as information technology facilities, technology (hardware, operating system software, telecommunication software, networking software, multimedia software), application software and business process and organisational structure. As result, numerous types of information technology architectures are possible depending on the extent of automation and combination of information technologies deployed. Hence, there cannot be any standard software for auditing all types of computerised environments that would enable achieving all the audit objectives. There are however generalized audit software products that can be used for a significant part of the audit procedures, however it would be the call of the auditor to ascertain the extent of use of such software in his audit work.

Irrespective of the IT environment, the auditor must have certain key competency areas:

- ▶ A through understanding of the fundamental concepts of Information Technology.
- ▶ Its key components and
- ▶ Functionality and limitations of such components
- ▶ Risks to the audit subject and controls thereof.

The auditor should gain relevant knowledge about computer hardware, operating systems, networking, database, application software, risks

and controls of a computerised environment and office automation software. These should be understood in terms of their impact as regards functionality, contribution and limitations and risks as regards the work of the auditor. Such knowledge would be a basic requirement before the auditor ventures into auditing in a computerized environment. If the auditor finds himself handicapped with requirement of advanced knowledge requirements as regards IS technologies and controls, it is possible for the auditor to rely on the services of an expert from the auditee organisation or more preferably an external expert.

IS Audit Approach

Auditing around the computer - Black box approach

Also known as the black box approach, audit around the computer refers to the concept of ignoring what is happening inside the computer and conducting the audit using the inputs and outputs as in manual audit. The objective of the auditor in this case is to understand and gain an assurance as to whether the IT systems, as regards his audit subject, are achieving the required controls or not. This he does by examining the inputs to the computer system(s) and analyzing the outputs from such system. If the output meets the pre-determined process and internal control requirements, then the auditor may conclude that the computer system does meet the required control expectations.

While using the black box approach the auditor verifies the existing systems and controls, not the processing of the computer applications. This enables the auditor to gain confidence as regards:

- ▶ Availability of correct and complete data for processing.
- ▶ Error detection and correction.
- ▶ Restart of compilation interrupted by power, mechanical or processing failures without duplicating the entries and records.
- ▶ Checks and controls for accuracy and completeness.
- ▶ Adequate data security against wrong processing, fraud, fire and other calamities.
- ▶ Prevention of unauthorized/invalid amendments, corrections and processing instructions (programs) operating instructions as sequences.
- ▶ Custody of the data files.

However the black box approach also suffers from significant disadvantages:

- ▶ The auditor can only gain reasonable satisfaction as regards a limited set of control objectives.
- ▶ Cannot be used where the audit subject involves complex logic and controls
- ▶ Cannot be used in a highly complex integrated controls environment such as an ERP environment

Auditing through the computer - White box approach

With the introduction of computerisation, traditional audit trails have disappeared. It is possible that the entire processing cycle occurs within the computer systems, with a single transaction that spans across organisational boundaries (such as vendors, agents etc). is completed by a complex set of networked computing systems. In many situations such as these and in case of ERP and e-commerce environments, hard copies of documents are generally not available.

It thus becomes necessary for the auditor to examine the logic and internal controls embedded in the application and related software. The auditor may also need to verify the technical accuracy of the systems, checks, controls, error detection and data security procedures. This would often require the auditor to use Information technology to achieve the auditing objectives effectively in such an environment; e.g. to examine the purchase cycle in an ERP environment, the auditor would need to use various computer assisted audit techniques such as extracting, analysing and querying on the transaction data to ascertain the effectiveness of controls, examining the parameter settings etc.

In such a situation, examination and testing of computer-implemented controls becomes mandatory for an auditor. In some cases, the high volume and complexity of transactions might necessitate the use of powerful IT tools. Computerised auditing techniques refers to the approach of reviewing the internal controls in the computerised environment, which usually involves the use of Computer Assisted Audit Techniques (CAATs). An understanding of the IT environment, its components and their operations is thus necessary. The objective is to understand the system and the processes and identify the risks and controls at the system or process level itself. This is essential lest weakness at the system or process should percolate to the activities level. Proficiency in computers becomes obligatory here. It is also essential to know the implications of how the controls are set up in the computerised environment at the various levels of hardware, operating system software, database, application software and access to these by the staff as per authorizations.

Computer Assisted Audit Techniques

Depending on the audit objective and approach to audit, the auditor would need to decide on the extent of computer assisted audit techniques. As explained earlier, the CAATs generally involve running the auditor's software under a controlled environment to verify the quality of data and controls in the computing environment. The auditor can potentially perform different kinds of tests, both addressing the compliance and substantive testing objectives, with the use of CAATs if the client's data is available to the auditor or the access to client's networks and IT resources are made available to the auditor. Hence CAATs are

helpful in collection of valuable audit evidence, analysis of client data to identify weaknesses and for reporting. Thereby the CAATs also enable the auditor to better manage his audit efficiently and qualitatively.

Need for CAATs

During the course of the audit an IS auditor should obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. The audit findings and conclusions have to be supported by appropriate analysis and interpretation of this evidence. Computerised information processing environments pose a challenge to the IS auditor to collect sufficient, relevant and useful evidence, since the evidence exists on magnetic media and can be examined only by using CAATs. With systems having different hardware and software environments, different data structure, record formats, processing functions, etc., it is almost impossible for the auditors to collect evidence and analyse the records without a software tool. Owing to resource constraints and the ever changing audit objectives it is almost impossible to quickly develop audit capabilities, without some sort of CAATs.

The ICAI Guidance note on CAAT describes CAATs as important tools for the auditor in performing audits. CAATs may be used in performing various auditing procedures including the following:

- ▶ Tests of details of transactions and balances, for example, the use of audit software for recalculated interest or the extraction of invoices over a certain value from the computer records
- ▶ Analytical procedures, for example, identifying inconsistencies or significant fluctuations
- ▶ Tests of general controls, for example testing the set-up or configurations of the operating system or access procedures to the program libraries or by using code comparison software to check that the version of the program in use is the version approved by management
- ▶ Sampling programs to extract data for audit testing
- ▶ Tests of application controls, for example, testing the functionality of a programmed control
- ▶ Re-performing calculations performed by the entity's accounting system.

However the auditor, while selecting the CAAT is faced with certain critical decisions that he may be required to make, while balancing on the quality and cost of audit:

- ▶ Use the audit software developed by the client
- ▶ Design and develop his own audit software
- ▶ Use a standard Off-the shelf Generalised Audit Software

The first two options require the auditor to be technically competent in programming and its methodology, which may not be his area of expertise. Computer audit software, also known as Generalised Audit

Module 7, Chapter 4

Programs (GAS) which are readily available and do not require for much expertise from the auditor can be used.

Types of CAATs

The various types of CAATs can be categorized as follows:

- a. Generalised Audit Software
- b. Specialised Audit software
- c. Utility Software

A brief description of the types of software is given below:

1. Generalised Audit Software (GAS)

Computer audit software may be defined as: “The processing of a client’s live files by the auditor’s computer programs”. Computer audit software may be used either in compliance or substantive tests. Generalised Audit software refers to generalized computer programs designed to perform data processing functions such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor. The use of Generalised Audit Software is perhaps the most widely known computer assisted audit technique. GAS has standard packages developed by software companies exclusively for auditing data stored on computers. These are economical and extensively used by auditors the world over. Available off the shelf, GAS can be used for a wide range of hardware, operating systems, operating environments and database. GAS generally achieves the most common data testing requirements which are common irrespective of the type of business or the kind of IT environment e.g. identifying cash payments in excess of the limits stipulated in the Income Tax Act, identification of pending receivables over 180 days, identifying ghost employees in payroll, identifying duplicate payments for supplier invoices, identifying employees with more than one login id etc.

2. Specialised Audit Software:

Specialised Audit software, unlike GAS, is written for special audit purposes or targeting specialized IT environments. The objective of these software to achieve special audit procedures which may be specific to the type of business, transaction or IT environment e.g. testing for NPAs, testing for UNIX controls, testing for overnight deals in a Forex Application software etc. Such software may be either developed by the auditee or embedded as part of the client’s mission critical application software. Such software may also be developed by the auditor independently. Before using the entity’s specialized audit software, the auditor should take care to get an assurance on the integrity and security of the software developed by the client.

3. Utility Software:

Utility software or utilities, though not developed or sold specifically for audit are often extremely useful and handy for conducting audits. These utilities usually come as part of office automation software, operating systems, database management systems or may even come separately. Utilities are useful in performing specific system command sequences and are also useful in performing common data analysis functions such as search, sort, appending, joining, analysis etc. Utilities are extensively used in design, development, testing and auditing of application software, operating systems parameters, security software parameters, security testing, debugging etc.

Generalised Audit Software

Of the above, the Generalised Audit Software are the most widely used for transaction audits and also for testing some systems controls. With their capabilities for achieving the traditional manual audit procedures in a highly effective and efficient manner, GAS products are an essential tool for every Chartered Accountant desiring to conduct a transaction or business controls audit. Hence it is important for the auditor to have detailed knowledge about the features, selection, functionality, limitations and audit approach with the use of GAS.

Typical Operations Using GAS

Generalised Audit Software (GAS) refers to standard software, which can directly read and access data from various database platforms, flat file systems and ASCII formats. This software has all the features of mathematical computations, stratification, statistical analysis, sequence check, duplicate check, re-computations, etc. Auditors can thus directly access the data stored in a computer and undertake various types of mathematical computations and statistical analysis. GAS cannot perform the audit but can facilitate selection and processing the information as per the clients' requirements. The two most commonly used GAS are ACL (Audit command Language) and IDEA (Interactive Data Extraction Analysis). Information about these packages can be accessed at www.acl.com and www.idea.com.

Typical operations using GAS include :

- ▶ Sampling-Items are selected following a value-based or random sampling plan.
- ▶ Extraction-Items that meet the selection criteria are reported individually.
- ▶ Totalling-The total value and number of items meeting selection criteria are reported.
- ▶ Ageing-Data is aged by reference to a base date
- ▶ Calculation - Input data is manipulated prior to applying selection criteria

Module 7, Chapter 4

- ▶ File comparison - A current version of a file for example, is compared with the previous year's version, or an input file is compared with a processed file.
- ▶ Production of circularisation letters.

Functional Capabilities of CAATs

CAATs facilitate auditors to use high-level problem solving software to invoke functions to be performed on data files. Typical functions of GAS which facilitate CAAT are :

- ▶ File Access - Helps to read different record formats and file structures.
- ▶ File Re-organisation - enables indexing, sorting, merging, linking with another file, etc.
- ▶ Data Selection - Facilitates global filtration conditions, selection criteria, etc.
- ▶ Statistical functions - Allows sampling, stratification, frequency analysis, etc.
- ▶ Arithmetical functions - Facilitates arithmetic operators and functions.

Typical Steps in using GAS

1. Define the audit objectives
2. Identify the tests that the package can undertake to meet the objectives.
3. Make out the package input forms for the tests identified.
4. Compile the package on the computer, clearing reported edit errors.
5. If a programmer has been adding coded routines to the package to fill out the input forms or to advise, the programmer's work must be tested.
6. Obtain copies of the application filed to be tested.
7. Attend the execution of the package against these copy files.
8. Maintain security of the copy files and output until the tests have been fully checked out.
9. Check the test results and draw audit conclusions.
10. Interface the test results with whatever subsequent manual audit work to be done.

Selecting, implementing and using CAATs

Computer Assisted Audit Techniques (CAATs) are a significant tool for auditors to gather evidence independently. CAATs provide a means to gain access and analyse data for a predetermined audit objective and to report audit findings with evidence. They help the auditor to obtain evidence directly on the quality of the records produced and maintained in the system. The quality of the evidence collected confirms the quality of the system processing.

CAATs Usage

CAATs could be used for various types of audit, which involve direct access, analysis and interrogation of data. Usage of CAATs can be broadly categorised as:

- ▶ Test of details of transactions and balances
- ▶ Analytical review of procedures.
- ▶ Compliance test of IS general controls
- ▶ Compliance test of application controls
- ▶ Penetration testing.

Advantages of using GAS

Independence of Data

The packages are independent of the data they retrieve and analyse. The user merely needs to define the data structures and specify simple selection criteria.

Portability of GAS and data

GAS can be installed on a PC or laptop and then used to run on live data on the computing environment of the client, by using the PC/Laptop as a dedicated audit terminal. It can be deployed for analysis on any personal computer. This feature facilitates easy extraction and analysis on any platform.

Analysis of data

The main purpose of such packages is to allow testing and analysis of data to achieve the control or audit objectives, with minimum knowledge of IT and specialised programming techniques. GAS usually have a GUI and very user friendly with menu driven command structure. Certain functions are automated to the extent that one command can carry out a fairly complex task—for example, the calculation of averages, means and other meaningful values. Fairly complex applications can be written, even to the extent of simulation of the processing of a particular business application running live, to enable the auditor or control professional to verify accuracy and completeness of the data processing and related controls.

Statistical Sampling

GAS is most commonly used in the selection of statistical samples for substantive testing. Various statistical functions and selection routines are automated and simple even for a non specialist.

CAATs - Effective usage methodology

The usage of CAATs will be effective if the following methodology is adopted

- ▶ Walk through the system and identify the areas of weakness.
- ▶ Perform compliance tests and evaluate the results.

Module 7, Chapter 4

- ▶ If the results necessitate substantive testing, use CAATs to get evidence.

Guidelines on decision factors for using CAATS

- ▶ When planning the audit, the IS auditor should consider an appropriate combination of manual techniques and CAATs.
- ▶ Computer knowledge, expertise, and experience of the IS auditor
- ▶ Availability of suitable CAATs and IS facilities
- ▶ Efficiency and effectiveness of using CAATs over manual techniques
- ▶ Time constraints
- ▶ Integrity of the information system and IT environment
- ▶ Level of audit risk.

Steps for effective use

Normally, audit conclusions and recommendations are based on the evidence collected by auditors. Audit conclusions based on incorrect and/or inappropriate evidences will reduce the credibility of the audit itself. Hence some of the steps associated with effective use of CAATs include:

- ▶ Set the audit objectives of the CAATs
- ▶ Determine accessibility and availability of organisation's IS facilities programs/systems and data.
- ▶ Define procedures to be undertaken (e.g. statistical sampling, recalculation, confirmation etc).
- ▶ Define output requirements
- ▶ Determine resource requirements, i.e., personnel, computers, CAATs, processing environment (Organisation's IS facilities or audit IS facilities)
- ▶ Obtain access to the organisation's IS facilities, programs/systems, and data, including file definitions.
- ▶ Document CAATs to be used, including objectives, high-level flowcharts, and run instructions.

Performance Steps

- ▶ Obtain written read-only access to IS facilities, systems and data
- ▶ Obtain file/table definition/structure
- ▶ Perform audit procedures using CAATs
- ▶ Review results obtained from CAATs to verify
- ▶ Perform reconciliation of data
- ▶ Check reasonableness of output
- ▶ Confirm logic, parameters and characteristics of data
- ▶ Document the steps undertaken

Cautions of use of CAATs

- ▶ Ensure integrity, reliability and security of the CAATs before selecting.

- ▶ Assure integrity of information Systems and security environment
- ▶ Assure the confidentiality and security of data as required by the client's
- ▶ Take into confidence client's IS staff of for usage of CAATs.

Use of Spreadsheets as an Audit tool

Spreadsheets are an effective and easy to use tool for the auditor to achieve audit and analytical procedures. Spreadsheets enable querying on a set of data based on the criteria and filters set by the auditor. Spreadsheets offer features which, though simple, can assist the auditor in efficient achievement of audit procedures. Many of the audit procedures for querying of transactions or for analyzing data relating to testing of controls require the auditor to define criteria. The subject data is tested against defined criteria. Some of these features include the following:

- ▶ **Join:** The data to be tested for a specified criteria may arise from more than one database. Hence this may require joining of files extracted from two or more different databases. Spreadsheets offer various features to joining and linking datafiles into single files.
- ▶ **Sort:** Sorting of subject data based on one or more data fields is often a requirement as part of various procedures to analyse trends, determine exceptions . Spreadsheets provide dialog boxes for simple to complex sorting functions
- ▶ **Filter:** Most spreadsheets provide for simple to very complex filtering of data based on multiple conditions or criteria, which is often useful in achieving searches based on complex audit criteria.
- ▶ **Summarise:** While working on large datafiles and working sheets, spreadsheets enable the summarizing of voluminous findings, relevant and useful for purposes of presentation.
- ▶ **Graphs and Charts:** Representation of findings using graphs and charts is extremely useful in conveying complex issues in a simple manner. Most spreadsheets provide a range of features that enable creating various types of graphs and charts, which can be linked to representative data.
- ▶ **Pivot Tables:** Pivot Tables are one of the most useful tools for data analysis since they allow multi-dimensional analysis of data.
- ▶ **Macros:** Where a series of spreadsheet menu-based command and instruction structures are required, macros enable repeated execution of long and complex instruction routines to be easily achieved using macro functions.

Risks associated with use of spreadsheets

The auditor should also be aware of the risks of using spreadsheets for analytical procedures and use of evidence arrived therefrom, e.g.:

- ▶ Errors in Input values leading to erroneous results

Module 7, Chapter 4

- Errors in logic and formulae leading to erroneous results
- Incorrect reference and range
- Problems associated with complex worksheets
- Improper or incorrect linking of worksheets
- Erroneous Overwriting of worksheets required for evidence

The auditor should institute adequate controls to safeguard his work against the above risks.

The following are some examples of CAATs, which can be used to collect evidence :

- ACL, IDEA etc.
- Utility Software such as Find, Search, flowcharting utilities
- Spreadsheets such as Excel
- SQL Commands, OS commands
- Third party access control software
- Application systems
- Options and reports built-in as part of the application/systems software
- Performance monitoring tools
- Network management tools, OS utilities
- High end CAATs
- RSAREF, DES, PGP
- TCP Wrapper, SOCKS, TIS Toolkit
- COPS, Tripwire, Tiger
- ISS, SATAN, etc.

Other Computer Assisted Audit Techniques

CAATs used in SDLC

Flowcharting Software

The processing logic of the programs may also be understood by examining the program flowcharts. This tool also calls for expertise in data processing. When writing a computer program, the programmer usually constructs a logic chart that is also useful, once the program is written, to assist in an appreciation of how the system works. This process can also help identify control procedures and system changes. Flowcharters are also useful in designing of audit software.

Test Data (test packs)

The use of audit test data (test packs) may be defined as: “The controlled application of an auditor’s test data (live or dummy) to client application program procedures”. The expression “test pack” is however, normally, reserved for situations where conventional testing is not practical (for example, where there is a loss of audit trail). A small sample of data is processed through the computer and the output is compared with manually generated output using the same data. It requires little computer

expertise, at least for simple batch systems. The auditor should take adequate care in designing the test pack and should be designed with the objective of making the application software fail.

Test Data generator

When test data or test packs are required to be generated, this may require a set of numerous data that tests a range within each parameter value. This requires a significant effort, if done manually. Test data generators are software packages which can be used either to construct data to be tested or to create dummy master files. The users describe the characteristics of the data required and the software generates a file of appropriate set of data and produces a listing. The data so generated can then be used as a “test pack”. Test data generators are cost effective especially, when large volumes of test data are needed for testing.

Program Comparison

This tool compares two different versions of the same program to ensure that they are identical. Software is available for this purpose both on the source code and the object code.

- ▶ A program implemented with the one tested and accepted by the user.
- ▶ Programs installed at different locations. Recompiling the source code and comparing them with the installed version.
- ▶ The presently installed version with a copy of the auditor’s previously tested version.

Program Code Analysis

Program code analysis also known, as program listing review is another tool, which can be used for analysis software code. A listing of the program code is obtained and reviewed for logic. Though not strictly a computer-assisted technique, program code analysis involves looking at the original instructions to the computer (the source program listing) to verify whether particular program procedures exist. Such findings are then corroborated using the test data. The technique is complex and requires a high level of technical skill for effective application.

Tracers

Tracing Software and utilities are extremely useful in understanding the trail of controls as they are executed by the various program lines in the application. Using a pre-determined or pre-identified set of input data, the tester or auditor can trace through the action of various instruction sets on the memory variable(s) marked for tracing.

Program (Parallel) Simulation

This consists of a separate computer application that performs the same functions as those used by the installed program. It uses the same data and files and the results are similar to those produced by the installed

Module 7, Chapter 4

program. Conceptually, it is akin to auditing around the computer. Parallel simulations may be done in any programming language. Using GAS non-technical persons can create parallel programs with little effort. Speed of execution is not a criterion, as the parallel simulation is done only on a one-off basis not as a regular production run. The objective is to test the adequacy of underlying controls that are expected to be embedded in the live computing environment. Parallel simulation is useful where the auditor may not have access to the live environment of the auditee.

CAATs used for systems testing

Utility Program

Most hardware manufactures provide software, known as “Utility programs”. They are designed to perform common tasks such as copying or sorting files or printing details of records for visual inspection. These programs may be useful in compliance or substantive tests. They may for instance, be employed to produce copies of data files required for interrogation purposes or to print out internal file labels, which can determine whether the correct file has been obtained.

Operating Systems and DBMS utilities

Auditors can also review the features of the operating systems and DBMS used so as to understand and use the powerful utilities to meet the requirements of auditors. In recent years, auditors have discovered that the powerful fourth generation languages contain many functions found in the GAS packages. Besides, they make it possible to download the needed data on to a microcomputer for further processing.

Statistical Techniques

Auditors may also consider using statistical procedures both for sampling items from a single database or shared databases. Some spreadsheet software contains a limited amount of statistical capability, but an auditor desirous of carrying out extensive statistical analysis may need software or an utility to do so.

Continuous Auditing Approach

Continuous auditing is a process through which an auditor evaluates the particular system(s) and thereby generates audit reports on real time basis. Continuous auditing approach may be required to be used in various environments. Such environments usually involve systems that are 24/7 mission-critical systems.

Enabling continuous auditing enables an independently developed or embedded set of audit software that continuously audits the transactions. The reports from such software provide real-time detection of au-

dit criteria and are capable of initiating or triggering corrective action before the risk gets out of control.

In the traditional method, the scope for market influence on the information contained in the audit report is less due to

1. The time gap between the audit and reporting
2. The deficiencies identified in the control systems can be rectified even by the management during the time gap.

Difference between continuous monitoring and continuous auditing

Continuous monitoring systems (CMS) enable organizations to monitor and obtain the information relating to systems, data types and process performance. For instance, the CMS developed to evaluate the accounts payable activities enables detection of double payments and details of such transactions by querying on invoice and related files

CMS is different from continuous auditing in the following manner:

1. Audit report: it does not generate any audit report.
2. Evidence: The opinion expressed in the report must be backed by substantive evidence and should be obtained from direct observation. The information gathered through CMS is indirect, as it is not obtained from direct observation. However, monitoring and testing the processes and systems by an IS auditor result in direct and independent monitoring under the control of the auditor.

Feasibility of Continuous Auditing

Continuous Auditing is generally not popular due certain problems associated with the implementation and management of continuous auditing techniques and tools:

- ▶ Risks of continuous auditing tools interfering with the integrity of application software running in live environment
- ▶ Continuous Auditing software may consume significant IT resources of the organisation thereby affecting the performance of IT for routine business functions, the impact of which may be felt by the customer ultimately
- ▶ Technological complexity associated with using such technologies.
- ▶ Cost of implementation of such techniques vs. the benefit

However feasibility of implementing continuous auditing systems would depend on the business risk that the auditee faces due to continuous process systems wherein an error or crime could get of control if not detected in a timely manner. Examples: an airline ticketing system may be applying significantly incorrect tariff to reservations, or, results of actions of hackers in online trading systems to defeat the controls of the systems for gains.

Techniques for Continuous Auditing

Snapshot

Most applications follow a standard procedure whereby, after taking in the user input they process it to generate the corresponding output. Snapshots are digital pictures of procedures of the console that are saved and stored in the memory. Procedures of the console refer to the application procedures that take input from the console i.e. from the keyboard or the mouse. These procedures serve as references for subsequent output generations in the future.

Typically, snapshots are implemented for tracing application software and mapping it. The user provides inputs through the console for processing the data. Snapshots are means through which each step of data processing (after the user gives the input through) is stored and recalled.

Let us consider, for example, a banking transaction. Numerous transactions are effected and processed by various application systems in a banking environment. While all applications are tested before being deployed, in an integrated computing environment, a cash withdrawal at the ATM may be processing by more than one software working in an integrated manner. In the event of some errors in transactions being detected or suspected, snapshot software installed as part of the production environment would continuously take pictures of transactions passing a particular control point e.g. instruction set executed in the memory of the ATM machine for processing withdrawal. Hence the error in code/ instruction can be pin-pointed and identified by the snapshot software.

Implementation

Specifically designed snapshot software applications or audit tools (incorporating snapshot software) are used for tracking the results of application of all or specified steps in the application process. The snapshot software takes a “digital image” of the user input and the corresponding intermediate state of results or output. Subsequently, digital images or snapshots taken by the snapshot software are stored in a separate file to be retrieved later. The digital images may also be distributed to selected servers and client systems for further processing. Snapshots may either be triggered manually by the User/Auditor by specifying the transactions in respect of which the snapshot needs to be taken or may be programmed to be triggered based on time or a occurrence of a particular event.

Snapshots are employed in the following:

- ▶ They are used for analysing and tracking down the flow of data in an application program, so as to know the underlying logic of the data-processing software.
- ▶ For documenting the logic, input/output controls (or conditions) of the application program and the sequence of processing.

Snapshots are generally deployed for tracking down the reasons for any disruption in the functioning of application or system software like operating system or database system.

Integrated Test Facility (ITF)

Integrated Test Facility (ITF) is a system in which a test pack is pushed through the production system affecting “dummy” entities. Hence this requires dummy entities to be created in the production software. For example, the auditor would introduce test transactions that affect targeting dummy customer accounts and dummy items created earlier for this testing purpose. The approach could also involve setting a separate dummy entity using the application software in the live environment. ITF is useful in identifying errors and problems that occur in the live environment and that cannot be traced in the test environment. However the disadvantage in using ITF is that the dummy transactions also append to the live database and hence will impact the results and reports drawn from the live database. It will therefore, be necessary to delete the test transaction from the system once the test is performed. As with all test packs, the output produced is compared with predicted results. This helps to determine whether the programmed procedures being tested are operating correctly.

System Activity File Interrogation

Most computer operating systems provide the capability of producing a log of every event occurring in the system, both user and computer initiated. This information is usually written to a file and can be printed out periodically. As part of audit testing of general controls, it may be useful for the auditor to review the computer logs generated at various points to build an audit trail. Wherever possible, unauthorised or anomalous activity would need to be identified for further investigation. Where a suitable system activity file is retained on magnetic media, one can select and report exceptional items of possible audit interest such as unauthorised access attempts, unsuccessful login attempts, changes to master records and the like.

Similar implementation is also possible by embedding special audit software in application software that maintains continuous transaction logs at various points in the application software. This technique is also referred to as the Systems Control Audit Review File. The files can be further analyzed to determine deviations and improper transactions.

Embedded Audit Facilities

Embedded audit facilities consist of program audit procedures, which are inserted into the client's application programs and executed simultaneously. The technique helps review transactions as they are processed and select items according to audit criteria specified in the resident code, and automatically write details of these items to an output file for subsequent audit examination.

This technique generally uses one or more specially designed modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the application system or program at points predetermined by the auditor. The auditor also determines the criteria for selection and recording. Automated or manual methods may be used to analyse the data later. This is intended to highlight unusual transactions, which can be later taken up for scrutiny.

Continuous and Intermittent Simulation

With significant advancements in technologies, business systems are increasingly driven by client-server systems with distributed computing and databases. The components of such systems are networked generally over geographically disparate locations. This has resulted in the need for auditing systems that not only enable continuous auditing of transactions but also have a low overhead on the IT resources of the auditee but without compromising on the independence of such systems. This has resulted in the use of continuous auditing techniques that the client-server environment to enable independent simulation of "suspect" transactions independently by the simulation audit software under the control of the auditor but using the on-line data of the auditee awaiting to be written to the database.

Annexure 1: ICAI Guidance Note on Computer Assisted Audit Techniques (CAATs)

Introduction

1. The overall objectives and scope of an audit do not change when an audit is conducted in a computer information systems (CIS) environment. The application of auditing procedures may, however, require the auditor to consider techniques known as Computer Assisted Audit Techniques (CAATs) that use the computer as an audit tool for enhancing the effectiveness and efficiency of audit procedures. CAATs are computer programs and data that the auditor uses as part of the audit procedures to process data of audit significance, contained in an entity's information systems.
2. The purpose of this Guidance Note is to provide guidance in the use of CAATs. This Guidance Note describes computer assisted au-

dit techniques including computer tools, collectively referred to as CAATs. This Guidance Note applies to all uses of CAATs when a computer of any type or size is involved whether that computer is operated by the entity or by a third party.

Description of Computer Assisted Audit Techniques (CAATs)

3. Computer Assisted Audit Techniques (CAATs) are important tools for the auditor in performing audits. CAATs may be used in performing various auditing procedures, including the following:
 - ▼ tests of details of transactions and balances, for example, the use of audit software for recalculating interest or the extraction of invoices over a certain value from computer records;
 - ▼ analytical procedures, for example, identifying inconsistencies or significant fluctuations;
 - ▼ tests of general controls, for example testing the set-up or configuration of the operating system or access procedures to the program libraries or by using code comparison software to check that the version of the program in use is the version approved by management;
 - ▼ sampling programs to extract data for audit testing;
 - ▼ tests of application controls, for example, testing the functioning of a programmed control; and
 - ▼ reperforming calculations performed by the entity's accounting systems.
4. CAATs allow the auditor to give access to data without dependence on the client, test the reliability of client software, and perform audit tests more efficiently. CAATs are computer programs and data that the auditor uses as part of the audit procedures to process data of audit significance contained in an entity's information systems. CAATs may consist of package programs, purpose-written programs, utility programs or system management programs. Regardless of the origin of the programs, the auditor substantiates their appropriateness and validity for audit purposes before using them. A brief description of the programs commonly used is given below.
 - ▼ **Package Programs** are generalized computer programs designed to perform data processing functions, such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor.
 - ▼ **Purpose-Written Programs** perform audit tasks in specific circumstances. These programs may be developed by the auditor, the entity being audited or an outside programmer hired by the auditor. In some cases, the auditor may use an entity's existing programs in their original or modified state because it may be more efficient than developing independent programs.

- ▼ **Utility Programs** are used by an entity to perform common data processing functions, such as sorting, creating and printing files. These programs are generally not designed for audit purposes, and therefore may not contain features such as automatic record counts or control totals.
- ▼ **System Management Programs** are enhanced productivity tools that are typically part of a sophisticated operating systems environment, for example, data retrieval software or code comparison software. As with utility programs these tools are not specifically designed for auditing use and their use requires additional care.

Details of some of the techniques used are mentioned in the Appendix.

Considerations in the Use of CAATs

5. When planning an audit, the auditor may consider an appropriate combination of manual and computer assisted audit techniques. In determining whether to use CAATs, the factors to consider include:
 - ▼ the IT knowledge, expertise and experience of the audit team;
 - ▼ the availability of CAATs and suitable computer facilities and data;
 - ▼ the impracticability of manual tests;
 - ▼ effectiveness and efficiency; and
 - ▼ time constraints.

Before using CAATs the auditor considers the controls incorporated in the design of the entity's computer systems to which CAAT would be applied in order to determine whether, and if so, how, CAATs should be used.

IT Knowledge, Expertise and Experience of the Audit Team

6. Auditing and Assurance Standard (AAS) 29, "Auditing in a Computer Information Systems Environment" deals with the level of skill and competence the audit team needs to conduct an audit in a CIS environment. It provides guidance when an auditor delegates work to assistants with CIS skills or when the auditor uses work performed by other auditors or experts with such skills. Specifically, the audit team should have sufficient knowledge to plan, execute and use the results of the particular CAAT adopted. The level of knowledge required depends on "availability of CAATs" and "suitable computer facilities".

Availability of CAATs and Suitable Computer Facilities

7. The auditor considers the availability of CAATs, suitable computer facilities and the necessary computer-based information systems and data. The auditor may plan to use other computer facilities when the use of CAATs on an entity's computer is uneconomical or impractical, for example, because of an incompatibility between the

auditor's package program and entity's computer. Additionally, the auditor may elect to use their own facilities, such as PCs or laptops.

8. The cooperation of the entity's personnel may be required to provide processing facilities at a convenient time, to assist with activities such as loading and running of CAAT on the entity's system, and to provide copies of data files in the format required by the auditor.

Impracticability of Manual Tests

9. Some audit procedures may not be possible to perform manually because they rely on complex processing (for example, advanced statistical analysis) or involve amounts of data that would overwhelm any manual procedure. In addition, many computer information systems perform tasks for which no hard copy evidence is available and, therefore, it may be impracticable for the auditor to perform tests manually. The lack of hard copy evidence may occur at different stages in the business cycle.
 - ▼ Source information may be initiated electronically, such as by voice activation, electronic data imaging, or point of sale electronic funds transfer. In addition, some transactions, such as discounts and interest calculations, may be generated directly by computer programs with no specific authorization of individual transactions.
 - ▼ A system may not produce a visible audit trail providing assurance as to the completeness and accuracy of transactions processed. For example, a computer program might match delivery notes and suppliers' invoices.
 - ▼ In addition, programmed controlled procedures, such as checking customer credit limits, may provide hard copy evidence only on an exception basis.
 - ▼ A system may not produce hard copy reports. In addition, a printed report may contain only summary totals while computer files retain the supporting details.

Effectiveness and Efficiency

10. The effectiveness and efficiency of auditing procedures may be improved by using CAATs to obtain and evaluate audit evidence. CAATs are often an efficient means of testing a large number of transactions or controls over large populations by:
 - ▼ analyzing and selecting samples from a large volume of transactions ;
 - ▼ applying analytical procedures; and
 - ▼ performing substantive procedures.
11. Matters relating to efficiency that an auditor might consider include:
 - ▼ the time taken to plan, design, execute and evaluate CAAT;
 - ▼ technical review and assistance hours;

Module 7, Chapter 4

- ▼ designing and printing of forms (for example, confirmations); and
 - ▼ availability of computer resources
12. In evaluating the effectiveness and efficiency of CAAT, the auditor considers the continuing use of CAAT application. The initial planning, design and development of CAAT will usually benefit audits in subsequent periods.

Time Constraints

13. Certain data, such as transaction details, are often kept for a short time and may not be available in machine-readable form by the time auditor wants them. Thus, the auditor will need to make arrangements for the retention of data required, or may need to alter the timing of the work that requires such data.
14. Where the time available to perform an audit is limited, the auditor may plan to use CAAT because its use will meet the auditor's time requirement better than other possible procedures.

Using CAATs

15. The major steps to be undertaken by the auditor in the application of CAAT are to:
- (a) set the objective of CAAT application;
 - (b) determine the content and accessibility of the entity's files;
 - (c) identify the specific files or databases to be examined;
 - (d) understand the relationship between the data tables where a database is to be examined;
 - (e) define the specific tests or procedures and related transactions and balances affected;
 - (f) define the output requirements;
 - (g) arrange with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made at the appropriate cut off date and time;
 - (h) identify the personnel who may participate in the design and application of CAAT;
 - (i) refine the estimates of costs and benefits;
 - (j) ensure that the use of CAAT is properly controlled;
 - (k) arrange the administrative activities, including the necessary skills and computer facilities;
 - (l) reconcile data to be used for CAAT with the accounting and other records;
 - (m) execute CAAT application;
 - (n) evaluate the results;
 - (o) document CAATs to be used including objectives, high level flowcharts and run instructions; and
 - (p) assess the effect of changes to the programs/system on the use of CAAT.

Testing CAAT

16. The auditor should obtain reasonable assurance of the integrity, reliability, usefulness, and security of CAAT through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed upon CAAT. The nature, timing and extent of testing is dependent on the commercial availability and stability of CAAT.

Controlling CAAT Application

17. The specific procedures necessary to control the use of CAAT depend on the particular application. In establishing control, the auditor considers the need to:
 - (a) approve specifications and conduct a review of the work to be performed by CAAT;
 - (b) review the entity's general controls that may contribute to the integrity of CAAT, for example, controls over program changes and access to computer files. When such controls cannot be relied on to ensure the integrity of CAAT, the auditor may consider processing CAAT application at another suitable computer facility; and
 - (c) ensure appropriate integration of the output by the auditor into the audit process.
18. Procedures carried out by the auditor to control CAATs applications may include:
 - (a) participating in the design and testing of CAAT;
 - (b) checking, if applicable, the coding of the program to ensure that it conforms with the detailed program specifications;
 - (c) asking the entity's staff to review the operating system instructions to ensure that the software will run in the entity's computer installation;
 - (d) running the audit software on small test files before running it on the main data files;
 - (e) checking whether the correct files were used, for example, by checking external evidence, such as control totals maintained by the user, and that those files were complete;
 - (f) obtaining evidence that the audit software functioned as planned, for example, by reviewing output and control information; and
 - (g) establishing appropriate security measures to safeguard the integrity and confidentiality of the data.

When the auditor intends to perform audit procedures concurrently with online processing, the auditor reviews those procedures with appropriate client personnel and obtains approval before conducting the tests to help avoid the inadvertent corruption of client records.

Module 7, Chapter 4

19. To ensure appropriate control procedures, the presence of the auditor is not necessarily required at the computer facility during the running of CAAT. It may, however, provide practical advantages, such as being able to control distribution of the output and ensuring the timely correction of errors, for example, if the wrong input file were to be used.
20. Audit procedures to control test data applications may include:
 - ▼ controlling the sequence of submissions of test data where it spans several processing cycles;
 - ▼ performing test runs containing small amounts of test data before submitting the main audit test data;
 - ▼ predicting the results of the test data and comparing it with the actual test data output, for the individual transactions and in total;
 - ▼ confirming that the current version of the programs was used to process the test data; and
 - ▼ testing whether the programs used to process the test data were the programs the entity used throughout the applicable audit period.
21. When using CAAT, the auditor may require the cooperation of entity staff with extensive knowledge of the computer installation. In such circumstances, the auditor considers whether the staff improperly influenced the results of CAAT.
22. Audit procedures to control the use of audit-enabling software may include:
 - ▼ verifying the completeness, accuracy and availability of the relevant data, for example, historical data may be required to build a financial model;
 - ▼ reviewing the reasonableness of assumptions used in the application of the tool set, particularly, when using modeling software;
 - ▼ verifying availability of resources skilled in the use and control of the selected tools; and
 - ▼ confirming the appropriateness of the tool set to the audit objective, for example, the use of industry specific systems may be necessary for the design of audit programs for unique business cycles.

Documentation

23. The various stages of application of CAATs should be sufficiently documented to provide adequate audit evidence.
24. The audit working papers should contain sufficient documentation to describe CAAT application, including the details set out in the sections below.

(a) Planning

- ▶ CAAT objectives;

- ▶ CAAT to be used;
- ▶ Controls to be exercised; and
- ▶ Staffing, timing and cost.

(b) Execution

- ▶ CAAT preparation and testing procedures and controls;
- ▶ Details of the tests performed by CAAT;
- ▶ Details of inputs (e.g., data used, file layouts), processing (e.g., CAATs high-level flowcharts, logic) and outputs (e.g., log files, reports);
- ▶ Listing of relevant parameters or source code; and
- ▶ Relevant technical information about the entity's accounting system, such as file layouts.

(c) Audit Evidence

- ▶ Output provided;
- ▶ Description of the audit work performed on the output;
- ▶ Audit findings; and
- ▶ Audit conclusions;

(d) Other

- ▶ Recommendations to the entity management; and
- ▶ In addition, it may be useful to document suggestions for using CAAT in future years.

Arrangements with the Entity

25. The auditor may make arrangements for the retention of the data files, such as detailed transaction files, covering the appropriate audit time frame.
26. In order to minimize the effect on the organization's production environment, access to the organisation's information system facilities, programs/systems and data should be arranged well in advance of the needed time period
27. The auditor should also consider the effect of these changes on the integrity and usefulness of CAAT, as well as the integrity of the programs/system and data used by the auditor.

Using CAATs in Small Entities

28. Although the general principles outlined in this Guidance Note apply in small entity IT environments, the following points need special consideration:
 - (a) The level of general controls may be such that the auditor will place less reliance on the system of internal control. This will result in greater emphasis on tests of details of transactions and balances and analytical review procedures, which may increase the effectiveness of certain CAATs, particularly, audit software.
 - (b) Where smaller volumes of data are processed, manual methods may be more cost effective.

Module 7, Chapter 4

- (c) A small entity may not be able to provide adequate technical assistance to the auditor, making the use of CAATs impracticable.
- (d) Certain audit package programs may not operate on small computers, thus restricting the auditor’s choice of CAATs. The entity’s data files may, however, be copied and processed on another suitable computer.

Appendix to the Guidance Note
Examples of Computer Assisted Audit Techniques

TECHNIQUES	DESCRIPTION	ADVANTAGES	DISADVANTAGES
AUDIT AUTOMATION	• Expert Systems • Tools to evaluate a client’s risk management procedures • Electronic working papers, which provide for the direct extraction of data from clients computer records • Corporate and financial modeling programs for use as predictive audit test	• These techniques are more useful when auditors are using laptops which can be directly linked with the entity’s system.	• Not applicable in the case of main-frame computers.
AUDIT SOFTWARE	Software used by the auditor to read data on client’s files, to provide information for the audit and/or to re-perform procedures carried out by the client’s programs.	• Performs a wide variety of audit tasks • Long term economies • Reads actual records • Capable of dealing with large volumes of transactions	• Requires a reasonable degree of skill to use • Initial set up costs can be high • Adaptation often needed from machine to machine

TECHNIQUES	DESCRIPTION	ADVANTAGES	DISADVANTAGES
CORE IMAGE COMPARISON	Software used by the auditor to compare the executable version of a program with a secure master copy	• Provides a high degree of comfort concerning the executable version of the program • Particularly useful where only executable versions are distributed	• Requires a high degree of skill to set up and to interpret the results • Where program have been recompiled the comparison may be invalidated as the program records everything as a difference • Printouts are hard to interpret and the actual changes made are difficult to establish • Availability restricted to certain machine types
DATABASE ANALYSERS	Software used by the auditor to examine the rights associated with terminals and the ability of users to access information on a database	• Provides detailed information concerning the operation of the database • Enhances the auditor's understanding of the database management system	• Requires a high degree of skill to set up and to interpret the results • Restricted availability both as regards machine types and database management systems • Specific and limited audit applicability

Module 7, Chapter 4

TECHNIQUES	DESCRIPTION	ADVANTAGES	DISADVANTAGES
EMBEDDED CODE	Software used by the auditor to examine transactions passing through the system by placing his own program in the suite of programs used for processing	• Performs a wide variety of audit tasks • Examines each transaction as it passes through the system • Operates continuously • Capable of identifying unusual transactions passing through the system	• There is a processing overhead involved because of the extra program • Definition of what constitutes an unusual transaction needs to be very precise • Precautions need to be taken over the output from the programs to ensure is security • Precautions need to be taken to ensure that the programs cannot be suppressed or tampered with • Requires some degree of skill to use and to interpret the results
LOG ANALYSERS	Software used by the auditor to read and analyse records of machine activity	• Provides detailed information on machine usage • Long term economics • Effective when testing integrity controls	• Requires a high degree of skill to use and to interpret the results • Limited availability as regards machine types • High volume of records restricts extent of test
MAPPING	Software used by the auditor to list unused programs instructions	• Identifies program code which may be there for fraudulent reasons	• Very specific objective • Requires a high degree of skill to use and to interpret the results • Adaptation needed from machine to machine

TECHNIQUES	DESCRIPTION	ADVANTAGES	DISADVANTAGES
MODELLING	A variety of software, usually associated with a microcomputer, enabling the auditor to carry out analytical reviews of client's results, to alter conditions so as to identify amounts for provisions or claims, or to project results and compare actual results with those expected	• Can be a very powerful analytical tool • Can enable the auditor to examine provisions on a number of different bases • Very flexible in use • Can provide the auditor with useful information on trends and patterns	• A high volume of data may need to be entered initially • Results require careful interpretation
ON-LINE TESTING	Techniques whereby the auditor arranges or manipulates data either real or fictitious, in order to see that a specific program or screen edit test is doing its work	• Very widely applicable • Easy to use • Can be targeted for specific functions carried out by programs	• Each use satisfies only one particular objective • Care must be taken to ensure that "live" data does not impact actual results
PROGRAM CODE ANALYSIS	An examination by the auditor of the source code of a particular program with a view to following the logic of the program so as to satisfy himself that it will perform according to his understanding	• Gives a reasonable degree of comfort about the program logic • The auditor can examine every function of the program code	• The auditor must understand the program language • The auditor needs to check that the source code represents the version in the source library, and that this version equates to the executable version

Module 7, Chapter 4

TECHNIQUES	DESCRIPTION	ADVANTAGES	DISADVANTAGES
PROGRAM LIBRARY ANALYSERS	Software used by the auditor to examine dates of changes made to the executable library and the use of utilities to amend programs	• Provides the auditor with useful information concerning the program library • Identifies abnormal changes to the library • Useful when testing program security	• Requires a high degree of skill to use and to interpret the results • Availability restricted to certain machine types • Only relevant when testing integrity controls
SNAPSHOTS	Software used by the auditor to take a “picture” of a file of data or a transaction passing through the system at a particular point in time	• Permits the auditor to examine processing at a specific point in time to carry out tests, or to confirm the way a particular aspect of the system operates	• Can be expensive to set up
SOURCE COMPARISON	Software used by the auditor to compare the source version of a program with a secure master copy	• Compares source code line by line and identifies all differences • Useful when testing integrity controls or particularly important program procedures	• Other procedures are necessary to ensure that the executable version reflects the source code examined • Requires some degree of skill to use and to interpret the results • Availability restricted to certain machine types

TECHNIQUES	DESCRIPTION	ADVANTAGES	DISADVANTAGES
TEST DATA - "LIVE", "DEAD", INTEGRATED TEST FACILITY OR BASE CASE SYSTEM EVALUATION	Fictitious data applied against the client's programs either whilst they are running or in an entirely separate operation. The results of processing the fictitious data are compared with the expected results based on the auditor's understanding of the programs involved	• Performs a wide variety of tasks • Gives considerable comfort about the operation of programs • Can be precisely targeted for specific procedures within programs • Long term economies	• "Dead" test data requires additional work for the auditor to satisfy himself the right programs were used • Care must be taken to ensure that "live" data does not impact actual results • Technique can be expensive to set up and cumbersome to use • Adequate for detection of major error but less likely to detect deep-seated fraud
TRACING	Software used by the auditor to identify which instructions were used in a program and in what order	• Helps to analyse the way in which a program operates	• There may be less costly ways to achieve the same objectives, although not in the same detail • Requires a high degree of skill to use and to interpret the results • Adaptation needed from machine to machine

Annexure 2: Sample Results of Using CAAT

Report on review of RDBMS data using SQL

As a part of our audit procedure, we have used SQL to directly access and analyse the data stored in the tables. Our observations and the related analysis are given below. These observations relate to the data stored, which could impact financial accounts. So we have submitted this information to statutory auditors and user department of ABC requesting them to verify these SQL results and confirm the impact on the financial statements. The detailed SQL statements can be obtained from the IT department of ABC. We have given a copy of this draft re-

port to ABC for confirmation of facts. Our observations with implications, comments and our risk assessment are given below :

1. Observation - High

Users available with invalid employee codes e.g. employee Code 15. There are two user IDs with user ID 15, which is still being used. Used by live users these transactions will not establish user accountability.

Implications

Since the employer code is invalid, it will be difficult to establish accountability for transactions entered using the ID in case of errors or frauds.

IT Department's feedback and agreed action

This User-ID was created during the time of data conversion. It has been disabled so that transactions cannot be entered using this.

2. Observation - High

- a) Past Employees having Id in access Table
19 users to have user IDs. Their employee Id and name are given so that a final list may be prepared with actual users who are expected to have access to the system.
- b) No. of transactions entered by each employee from the inception
This table has the number of transactions entered by each employee. Some users have entered only 4 transactions while some others have entered more than 30,000 transactions. This needs to be analyzed.

Implications

The number of user accounts in the system is much more than the actual users. This is because past and temporary users have not been disabled.

IT Department's feedback and agreed action

The number of users will correspond to the actual users. All other users will be disabled.

3. Observation - High

Transactions with amount as null Transactions with null amount are listed day-wise. There are 181 transactions, which need to be analyzed.

Implications

This results in dummy transactions, which may not have any value, or genuine transactions might have been stored without values.

IT Department's feedback and agreed action

Such action is taken in cases where DD charges are deducted from the loan amount for obtaining DD but the loan account is debited with the total amount including DD charges. This does not have any financial

impact. The feedback derived from the IT department leads to agreed action.

4. Observation - Low

UNITS HAVING REBATE AS 3% IN LOAN COMTABLE OF HO.

There are 69 accounts with a total rebate of Rs.4,12,132. These need to be confirmed.

Implication

There could be excess rebate granted for loan accounts.

IT Department's feedback and agreed action

All the listings are of genuine accounts where the rebate is 3%

5. Observation - HIGH

Total number of accounts where penal interest is more than 2.5%

- i) There are a number of accounts with penal interest ranging from 2% to 23.5%. The number of transactions as per interest rate is given elsewhere. Detailed account-wise transactions were extracted, verified and confirmed. There are 34 categories of interest computations, which were given separately to the users.

- ii) Accounts having penal rates as '0' as on 10-Mar-2000.

There are 196 transactions listed unit-wise with zero panel interest rate.

Implication

The interest computation is wrong in that there are errors in the panel interests. Also there is no control on modification to these rates.

IT department's feedback and agreed action

Incorrect past data is being rectified and further controls are being incorporated in the programs to ensure that all modifications to such master tables are captured and also authorised. These will also be printed as exception report.

6. Observation - HIGH

Voucher No. is Null

In a few cases the voucher number is null date	Voucher No.
22 April 2000	31
23 June 2000	67
14 July 2000	18

Implication

The transaction may not be picked up for processing as the voucher number is provided by the system. Such errors could have occurred due to program bugs.

IT department's feedback and agreed action.

Voucher numbers are not used for generating any reports. However, they will be investigated and rectified.

7. Observation - Low

Sanction Amount is Zero

The sanction amount for 26 cases is zero.

Implication

The past data has not been captured and invalid data is printed in the statement of accounts.

IT department's feedback and agreed action.

These are being identified and rectified as one-time measures. Appropriate controls will be built into the program.

8. Observation - HIGH

Account with loan balance and principal balances is zero but interest balance and other debits is not zero.

There are genuine cases where unit has been taken over and the amount realised is credited towards principals. Only if there is a balance of loan left is it transferred to interest and other debits.

Implication

There may be errors on account of data entry because of invalid data and incorrect statement of accounts.

IT department's feedback and agreed action

All cases, which are not genuine are being identified and rectified as one-time measures. Appropriate controls will be built in the program to consider them as a separate account type.

Summary

Audit in a computerized environment could require either audit of transactions and records or audit of IT and general controls IT Environment impact on Audit Methodology. The auditor should gain good understanding of the technology environment and the state of related controls before designing his audit procedures. Traditional techniques of auditing may not be effective in achieving even the conventional audit objectives in a computerized environment. Hence it is pertinent that the auditor should take into consideration the risks in the computerized environment and choose the appropriate audit approach, computer assisted audit techniques and methods for accomplishing his audit objectives. This requires a good understanding on the part of the auditor in understanding the various types, advantages and risks of using general and special audit tools and techniques and should possess the necessary skill and competence to audit in a computerized environment. Where the auditor encounters continuous computer processing environments, the auditor should evaluate the audit objective requirements taking into

consideration the nature of automated processing and apply the most appropriate continuous auditing technique. Hence auditor uses his knowledge and expertise in assessing the risks in the computerized environment, and possess expertise in choosing the appropriate audit approach and audit techniques for effective completion of audit.



5 Overview of Information Systems Audit and Related Standards

Learning Goals

To provide an understanding of national and international Audit Standards, and related areas such as certification and regulatory developments

Audit Standards

Every profession has a unique repository of knowledge, which lends credence to its specialization. This knowledge often forms the basis to define commonly accepted practices. Very often the technical competencies and skills of professionals are assessed against these practices. So the first step towards becoming a specialized professional is to gain a thorough understanding of these matters. IS auditing standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively.

The audit work entrusted to the auditor may involve either achieving traditional audit objectives in a computerized environment or information systems audit objectives. In either case, the chartered accountant, at the time of planning and carrying out his audit should take into consideration the impact of the auditing and assurance standards (AAS) issued by the Institute of Chartered Accountants of India, while designing his audit procedures.

AAS 27 – Auditing and Assurance Standard on Auditing in a computer information systems environment

AAS 27 issued by ICAI establishes standards on procedures to be followed when an audit relating to accounting information is conducted in a computer information systems environment. The pronouncement outlines the procedures that an auditor entrusted with financial, operational or other conventional audit objective relating to accounting information should carry out while auditing in a computerized environment.

AAS 27 requires the auditor to consider the effect of a CIS environment on his audit and discusses the risks and caution that an auditor should

Module 7, Chapter 5

exercise while carrying out his traditional audit objectives in a computer information systems environment and elaborates on the following:

- ▶ The auditor's responsibility in gaining sufficient understanding and assurance on the adequacy of accounting and internal controls that protect against the inherent and control risk in a CIS and the resulting considerations to be taken while designing his audit procedures.
- ▶ The potential impact of auditing in a CIS on the assessment of control and audit risk.
- ▶ The auditor is required to determine the following factors to determine the effect of CIS environment on the audit arising from
- ▶ The extent to which the CIS is used for recording, compiling and analyzing accounting information.
- ▶ The system of internal controls relating to the authorized, complete, accurate and valid processing and reporting procedures.
- ▶ The impact of the CIS accounting system on the audit trail
- ▶ The Standard also requires the auditor to have sufficient knowledge of the CIS and possess appropriate specialized skills to enable him to plan, direct, supervise, control and review the work performed.

The text of AAS 27 can be found at the end of this chapter.

IS Audit Guidelines By ISACA

Information System Audit and Control Association (ISACA) has issued standards, procedures and guidelines for IS Auditing. These provide mandatory procedures, guidance and procedures for IS auditing. IS control professionals should use their professional judgment when applying the standards, and provide justification (if any) for the departure from the standards.

ISACA IS Auditing Standards

1. Audit Charter
2. Independence
3. Professional Ethics and Standards
4. Competence
5. Planning
6. Performance of Audit Work
7. Reporting
8. Follow Up Activities

ISACA IS Auditing Procedures

1. IS Risk Assessment
2. Digital Signatures
3. Intrusion Detection
4. Viruses and Other Malicious Logic
5. Control Risk Self Assessment
6. Firewalls
7. Irregularities and Illegal Acts

ISACA Audit Guidelines

1. Using the Work of Other Auditors
2. Audit Evidence Requirement
3. Use of Computer Assisted Audit Techniques (CAATs)
4. Outsourcing of IS Activities to Other Organisations
5. Audit Charter
6. Materiality Concepts for Auditing Information Systems
7. Due Professional Care
8. Audit Documentation
9. Audit Considerations for Irregularities
10. Audit Sampling
11. Effect of Pervasive IS Controls
12. Organisational Relationship & Independence
13. Use of Risk Assessment in Audit Planning
14. Application Systems Review
15. Planning
16. Effect of Third Parties on an Organisation's IT Controls
17. Effect of Nonaudit Role on the IS Auditor's Independence
18. IT Governance
19. Irregularities and Illegal Acts
20. Reporting
21. Enterprise Resource Planning (ERP) Systems Review
22. Business-to-consumer (B2C) E-commerce Review
23. System Development Life Cycle (SDLC) Review
24. Internet Banking
25. Review of Virtual Private Networks
26. Business Process Reengineering (BPR) Project Reviews

COBIT – IT Governance Model

A. Objective

COBIT (Control Objective for information and Related Technology) is a one-stop reference point of current preferred practices for IS control practitioners. It is a collection of generally accepted auditing practices (control objectives for an IT environment). 36 Sources were used to develop COBIT, making it the most comprehensive standard.

COBIT is used as a benchmark by IS control specialists to assess how an activity is practised or implemented. Auditors have to provide the management and business process owners of the organisation a reasonable assurance that relevant control objectives are being met; identify where there are significant weaknesses in those controls; substantiate the risk that may be associated with such weaknesses; and finally, advise these executives on the corrective actions that should be taken.

B. Audience

COBIT is a multi-purpose tool, which has been jointly developed by the information systems Audit and Control Foundation, several major sponsors and technology consultants. It can be used by:

- ▶ Management, to balance risk and control IT investment and to benchmark the existing and future IT environment.
- ▶ Users, to obtain assurance on security and control of products and services they acquire.
- ▶ Auditors, to substantiate opinions to management on internal controls and advise on the necessary minimum controls.

Open Standard

COBIT is an open standard that can be downloaded on a complimentary basis from the IT Governance Institute in affiliation with the Information Systems Audit and Control Association (ISACA) at www.isaca.org. It is the outcome of years of research and cooperation among global IT and business experts. It provides an authoritative, globally accepted set of IT practices for business managers and auditors. COBIT is accepted and used worldwide as the breakthrough IT governance tool that helps in understanding and managing IT - related risks.

COBIT is based on the Information Systems Audit and Control Foundation's (ISACF) control objective. It has been enhanced to meet existing and emerging international technical, professional, regulatory and industry-specific standards. The resulting control objectives have been developed for applications in organisation-wide enterprise information systems. COBIT's best practices (consensus of experts) help in optimising information investment, but better still it helps in proactively assessing and managing risks.

Tool Kit

COBIT consists of the following components each with its own objective:

- ▶ The **executive summary** is designed to provide key concepts in IT governance.
- ▶ The **framework** is a conceptual model linking control objectives to business objectives
- ▶ The **control objectives** provide the landscape of the IT Environment
- ▶ The **audit guidelines** make it easy for the auditor to navigate through any IS environment
- ▶ The **implementation tool** set makes it easy to get started on the audit.
- ▶ **Management guidelines** provide tools for benchmarking processes.

Application of COBIT for IS Audit

COBIT has four domains with 34 IT processes and 318 specific and detailed control objectives. The detailed control objectives can be used to

evaluate the available controls in an organisation. The IS auditor can base his audit approach, findings and recommendations on COBIT.

It provides a macro business perspective, and then focuses on the need for deploying IT, aligning IT and business objectives, ensuring IT governance and the methodology for management, users and auditors.

Control objectives are the most important aspect of an IS audit as they provide the minimum level of controls required. These objectives have to be developed keeping in mind the requirements of various business and technical environment. Generally, control objectives are meant for the management and staff of the IT, control and audit functions. More importantly, it's for the business process owners. Control objectives provide precise and clear definitions of a minimum set of controls. This ensures effectiveness, efficiency and economy in utilising resources before commencing the audit. For each IT process to be audited, detailed control objectives are to be identified as the minimum set of controls benchmarks which need to be in place. Existing controls in the audited environment can then be assessed to verify their sufficiency.

Other Global Standards on IS Assurance and Audit

A. BS7799 Standard of the British Standards Institute

British Standard (BS) 7799 was first published in 1995 to provide a comprehensive set of controls that consisted of the best practices in information security. The standard was revised in 1999 and again in 2002. The standard is published in two parts:

BS 7799-1 Part One: Code of Practice for Information Security Management

BS7799-2 Part Two: Specification for Information Security Management Systems

Part One is also referred to as BS ISO/IEC 17799 or ISO 17799. Part Two continues to be referred to as BS 7799-2. The BS7799-2-2002 is based in the Plan-Do-Check-Act model and recommended the management process required to build, operate, maintain and improve an ISMS. The ultimate goal of BS7799 is to provide a development plan on which the information security management system could be built. The standard was written to cross all boundaries, regardless of sector, size of organisation and structure.

ISO 17799 is intended to provide a single reference point for the wide range of controls required for most situations where IT is used in industry, commerce and communication. This security is divided into 10 key sections:

1. Information Security Policy
2. Organisation of assets and resources

Module 7, Chapter 5

3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Systems Development and Maintenance
8. Access Control
9. Business Continuity Management
10. Compliance

B. SAS 70 - Statement on Auditing Standards (SAS) No. 70, Service Organizations (AICPA)

In the present global business environment, outsourcing of business processes or activities is an increasingly common practice. Therefore, service organisations must also be able to assure on the adequacy of controls and safeguards when they host or process data belonging to their customers. The services could be any services such as data processing, sales or payroll processing, applications and claims processing, IT management, data center operations and management, application service providers, etc.

Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).

SAS 70 audit involves an in-depth audit of the service organisation's control activities, which generally include controls over information technology and related processes. SAS 70 also specifies a standard format of report, which signifies that the auditor has examined the service organisation control objectives and control activities. The auditors conducting the examination and issuing the report are referred to as the service auditors. The service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting.

SAS 70 provides for two types of reports called Type I and Type II reports. A Type I report describes the service organization's description of controls at a specific point in time, whereas a Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a period of time.

SAS 70 is an auditing standard, which enables an independent auditor to evaluate a service organization's controls. The audit report (i.e. the service auditor's report) contains the auditor's opinion; a description of the controls in place; and a description of the auditor's tests of operation effectiveness.

If the report is of Type II, then it can be shared with the service organization's customers (user organizations) and their respective auditors

(user auditors). The service organization is responsible for describing its control objectives and activities that are relevant to user organizations and their auditors.

C. SysTrust

The SysTrust service is an assurance service that has been jointly developed by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). It is designed to increase the comfort level of management, customers, and business partners with systems that support a business or particular activity. In a SysTrust engagement, the practitioner evaluates and tests whether or not a specific system is reliable when measured against four essential principles availability, security, integrity and maintainability. Here is a brief explanation of the four key SysTrust principles:

1. **Availability:** The system is available for operation and use at times set forth in service-level statements or agreements.
2. **Security:** The system is protected against unauthorized physical and logical access.
3. **Integrity:** The system processing is complete, accurate, timely, and authorized.
4. **Maintainability:** The system can be updated when required without adversely affecting its availability, security and integrity.

A detailed criterion exists for each of the above principles. The SysTrust criteria are posted on both the AICPA and CICA web sites.

At the completion of a SysTrust engagement, the practitioner renders an opinion on the management's assertion (or the actual subject matter) that effective controls have been maintained. The practitioner can report on all four SysTrust principles together, or on each principle separately. Because the SysTrust principles and criteria are established and available to any user, the practitioner's report does not have to be restricted to specific parties.

D. IT Infrastructure Library (ITIL)

With organisations increasingly dependent on Information Technology for running their business, there is need for high quality of IT services. Hence the process underlying IT services and IT Service Management has come into focus. ITIL or the IT Infrastructure Library is a series of documents that provide a framework for implementation of IT Service Management.

ITIL was originally created by the CCTA, a UK Government agency. It has come to be recognized as the de facto standard for best practice in the provision of IT service. ITIL aids a framework based approach to structured IT service management, which can be customized by organisation to suit their needs. ITIL provides through a series of documents, a

Module 7, Chapter 5

set of best practices further supported by a comprehensive qualifications scheme, accredited training and implementation and assessment tools, thus enabling benchmarking of IT Service Management maturity across organisations and against standards. ITIL enables an organisation to get certified against the Standard for IT Service Management (BS15000), a product of the British Standards Institute.

ITIL deals with a detailed understanding of the IT service management processes and IT service support processes and IT Service Delivery Processes.

Some of the topics covered as part of ITIL are:

- IT Service support processes
- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management
- IT Service Delivery processes
- Service Level Management
- Help Desk Management
- Disaster Recovery Planning/IT Service Continuity Management
- Capacity Management
- Financial Management
- Availability Management
- Security Management

Overview of IT Certification

A. ISO 9000 family of standards

ISO is the International Organization for Standardization. It is made up of about 140 national standards institutes from countries, large and small, in all regions of the world. It develops technical standards, which serve to safeguard consumers and general users of products and services.

ISO 9000 is a family of standards that address quality management systems within an organization. When an organization has a management system that is ISO 9000 certified - this means an independent auditor has checked the processes influencing quality and it conforms to the standard requirements. The primary objective is to give the management of an organization and its customers confidence that it is in control of the way it does business. An organization that engages an independent auditor or certification body to check their processes receives a certificate of conformity from the auditor/ certification body.

ISO 9000 lays down standards that an organization's quality system must meet; but it does not dictate how they should be met. Revisions

to the ISO 9000 family of standards occurred in late 2000 to reduce the number of standards; provide more explicit requirements for achieving customer satisfaction and continual improvement ; provide a more logical structure and provide the definition of eight universal quality management principles.

B. Overview of ISO 9001:2000

The highlight of the ISO 9001:2000 international standard is that, it emphasises the principles of Management and Measurement of Performance in all spheres within the industry. In this context, now the term “Quality System’ has changed to Quality Management System’ (QMS), and is moving towards at Management Oriented Quality System.

ISO 9001 and ISO 9004 are referred to as the ‘consistent pair’. They link modern quality management to the processes and activities of an organization. This includes a focus on continual improvement and customer satisfaction to ensure global applicability. The chief factors for the revision process are:

- ▶ Applicability to all product categories and to all sizes of organizations.
- ▶ Move towards a format and language that is clear, readily translatable and easily understandable.
- ▶ Ability to connect QMS to organizational processes.
- ▶ Provision of a natural stepping - stone towards Total Quality Management.
- ▶ Greater orientation towards continual improvement and customer satisfaction.
- ▶ Compatibility with other management systems, such as ISO 14000 for Environmental Management.
- ▶ Provision of a consistent basis to address the primary needs and interests of organizations in specific sectors such as aerospace, automotive, medical devices, telecommunications and others.

There is a general apprehension that implementing ISO involves requires a lot of documents. ISO 9001 however stresses on ‘documented quality management system’ and not a ‘system of documents’. In reality, ISO 9001-2000 has significantly reduced the documentation requirements, and is considerably less prescriptive than the 1994 standard. It provides more flexibility to an organization in documenting its QMS. This enables each individual organization to develop and decide on the minimum amount of documentation required to demonstrate the effective planning, operation and control of its processes, it also helps to demonstrate the effectiveness and continual improvement of the effectiveness of its QMS.

Module 7, Chapter 5

Current ISO 9000 certificate holders will have up to three years to make the transition to the new version of ISO 9001.

Management Principles

ISO 9001 :2000 is based on eight management principles. Senior management can use this framework to guide their organizations towards improved performance. These principles also help organizations to achieve their quality objectives.

Principle 1 - Customer focus

Organizations should understand current and future customer needs and strive to meet them. They have to exceed customer expectations.

Principle 2 - Leadership

Leaders need to be clear about the vision and the mission of the organization. They should create and maintain an environment that fully involves the employees in achieving organizational objectives.

Principle 3 - Involvement of people

People at all levels have to be involved, so that the collective effort can be used for the organization's benefit.

Principle 4 - Process approach

The corporate objectives can be achieved more efficiently when activities and related resources are managed as a process.

Principle 5 - System approach to management

Identifying, understanding and managing interrelated processes as a system so that it improves the organization's effectiveness and efficiency.

Principle 6 - Continual improvement

Continual improvement of the organization's overall performance should be a permanent objective.

Principle 7 - Factual approach to decision making

Effective decision ought to be based on the analysis of data and information

Principle 8 - Mutually beneficial supplier relationships

An organization and its suppliers are interdependent and a mutually beneficial relationship will enhance the ability of both to create value.

The revision of the ISO quality management standards includes a significant change to the structure of ISO 9001 and ISO 9004. While retaining the essence, the new standard will re-position the 20 elements of the current ISO 9001:1994 and the guidelines of ISO 9004-1:1994 into following main sections

Quality Management System

This includes general quality system requirements with a process approach and related documentation requirements.

Management Responsibility

This includes Management Commitment, Customer Focus, Quality Policy, Planning (Quality Objectives), Responsibility, Authority and Communication and finally Management Reviews.

Resource Management

This includes provision of Resources, Human Resources, Infrastructure and work environment.

Product Realisation

This includes planning of and for Product Realisation, Customer - related Processes, Design and Development, Purchasing, Production and Service Provision and Control of Monitoring and Measuring Devices.

Measurement, Analysis and Improvement

This includes general points like Monitoring and Measurement of Data, Control of Non-conforming Products, Analysis of Data, Improvements using Corrective and Preventive Actions.

Most new users obtain measurable benefits early in the process of deploying these standards in business processes. These initial benefits must be sustained through effective internal auditing and management review of system performance. The nature of the business will determine how the standards have to be applied to achieve the stated objectives.

Based on the ISO criteria, auditors can test the conformity of a product to its initial specifications. ISO 9126 is the documented standard for software development and system documentation.

C. Overview of Capacity Maturity Model (CMM)

In September 1987, the Software Engineering Institute (SEI) released a process maturity framework and a maturity questionnaire to the industry. These were tools for identifying to identify areas of improvement that an organisation needed in its software processes within an organisation. Based on the process maturity framework and the response to the questionnaire, the SEI evolved the Capability Maturity Model (CMM). SEI is a US Department of Defence (DOD) funded organisation set up in 1983 and located at Carnegie Mellon University. Its mission is to provide leadership in advancing the state of the practice of software engineering to improve the quality of systems that depend on software.

According to SEI, improvements in software are possible only if processes are available to build the products. A software process is defined

Module 7, Chapter 5

as a set of activities, methods, practices and transformations that people use to develop software (activities involved in requirement analysis design and the like) and associated products viz. project plans, documents and the like. Software Process capability describes the range of expected results that can be achieved by following a software (SW) process.

The SW process capability of an organisation provides a way of predicting the most likely outcomes to be expected for projects that an organisation undertakes. Examples of expected results / likely outcomes are normally in terms of quality (e.g. no. of delivered defects / LOC), productivity (e.g. LOC / person-month) etc.

Software Process Maturity is the extent to which a specific process is explicitly defined, managed, measured controlled and is effective. The capability maturity model provides SW organisations guidance on how to control the SW processes, and how to evolve towards a culture of SW engineering and management excellence. It defines several evolutionary steps to achieve these goals.

A maturity level according to CMM is a well-defined evolutionary stage and provides a layer in the foundation for continuous process improvement. Each level comprises a set of goals, that when satisfied, stabilises an important component of the SW process (e.g. estimation project planning and the like). Achieving each level results in an increase in the process capability of an organisation. There are five levels defined by CMM. If they are achieved it results in continuous process improvement within organisation.

CMM Levels

In the CMM, each level has several key process areas (KPAs). A KPA is a focus area for improvement. For example, project planning, project tracking and configuration management are focus areas at level 2. Each KPA has certain key practices, which are classified under the following categories.

- ▶ **Commitment to Perform:** CMM states that the organisation should have a policy that provides direction to ensure that KPA goals are met.
- ▶ **Ability to Perform:** Appropriate training, funding and infrastructure are made available to projects.
- ▶ **Activities:** The activities that have to be performed to satisfy the KPA.
- ▶ **Measurement and Analysis:** The measurements that need to be made to track the status of a project with regard to the KPA.
- ▶ **Verifying Implementation:** Checks (e.g. audits, management reviews) that should be performed to ensure that the KPA is satisfied

Characteristics of organisations at each level

Level 1 : Initial

In this level, the SW process is characterised as adhoc, and occasionally even chaotic. Few systematic processes are defined, and success depends on individual effort. Level 1 has no KPAs. Level 1 indicates that the organisation is operating without well-defined processes in place.

Level 2 : Repeatable

Basic project management principles are established to track cost, schedule and check functionality. The necessary process discipline is in place to repeat earlier success on projects with similar applications using practices from past projects.

Level 3 : Defined

The SW process for both management and engineering activities is documented, standardised and integrated into a standard SW process for the organisation (e.g. maintenance process, configuration management process). All projects use approved and tailored versions of the organisation's standard SW process(es) for developing and maintaining SW. Projects use historical information and experiential knowledge for planning and executing projects. Data and information from projects is regularly and systematically collected and organised (process database and process assets) so that the same can be reused by other projects.

Level 4 : Managed

Detailed measures of the SW process and product quality and established and performed. Both the SW process and products are quantitatively understood and controlled. Examples of process measures are defect removal, efficiency of reviews and tests. Example of a measure of product quality is # of defects / LOC. Projects establish goals for quality and control execution using data to meet the goals.

Level 5 : Optimising

Continuous process improvement is enabled by quantitative feedback from the process, and from piloting innovative ideas and technologies. Defects prevention is performed at the project and organisation level. Change in technology is initiated only after a detailed evaluation of cost benefit in a planned way. Processes are evaluated and change similarly initiated. In short, the impact of any change in process or technology is clearly understood in quantitative terms. At level 5, the organisation clearly understands the impact of introducing a testing tool or a CMM tool in similar projects.

D. Capability Maturity Model-Integrated (CMMI)

CMMI or Capability Maturity Model Integration, developed by the Software Engineering Institute, is a model for improving and appraising the performance of development organizations. The CMM (the original

Module 7, Chapter 5

version of the CMMI) was originally commissioned by the American Department of Defence to help them qualify software vendors' capabilities. From there it quickly evolved into a powerful tool to guide process improvement initiatives, not only for Software Development but for many related fields such as Systems Engineering, Product Acquisition, Team Management, Research and Development, etc.

CMMI is a model based process improvement method. The CMM was originally published in 1993 as a Software Maturity Model. The CMMI is a natural evolution from the CMM which has moved from Software focus to multi disciplinary focus.

The generic model components under CMMI are:

- 0- Incomplete
- 1- Performed
- 2- Managed
- 3- Defined
- 4- Quantitatively Managed
- 5- Optimising

The process area groupings under CMMI are:

- ▶ Project Management
- ▶ Process Management
- ▶ Engineering
- ▶ Support

The model also provides for two architectural structures, which the organisation can choose from:

- ▶ Staged
- ▶ Continuous

The continuous model allows the organisation to select the order of improvement process areas that best meets the organisation's business objectives and mitigates the organisation's areas or risk.

Whereas the stages model provides a proven sequence or improvements starting with the basic management practices to successive levels, which steps into the next level. However both staged and continuous architectures are designed to deliver equivalent results.

SSE CMM

Systems Security Engineering Capability Maturity Model is a variation of the CMM that focuses on the security engineering process areas.

The model describes the essential characteristics required to ensure good security engineering practices of an organisation's security engineering process. SSE CMM applies to developers and integrators of secure products and also to all types of organisations that provide security services and security engineering.

The model describes the various stages of the life cycle of a security product or secure system life cycle. These stages include concept definition, requirements analysis, design, development, integration, installation, operations, maintenance and decommissioning.

SSE CMM serves the following purposes:

- ▶ Provides a tool for evaluating security engineering practices and define improvements
- ▶ A standard against which customers can evaluate the service provider's capability as regards secure products and services
- ▶ Serves as a self improvement model for helping developers of secure products and security service providers, to build confidences and assurances.

Overview of Regulatory Developments Impacting Controls in a Computerized Environment

A. Information Technology Act, 2000

The Information Technology Act (the IT Act or the Act) was enacted on 7th June 2000, to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to e-commerce and to promote efficient delivery of Government services by means of reliable electronic records (commonly referred to e-governance). The IT Act is modeled on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law, which brings uniformity to the law applicable to alternatives to paper based methods of communication and storage of information.

With the traditional legal structure in India, thus far, supporting paper-based methods of communication, the IT Act amends the Indian Penal code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

The act does not apply to the following:

- ▶ A negotiable instrument as defined in Section 13 of the Negotiable Instruments Act, 1881.
- ▶ A power of attorney defined in section 1A of the Powers of Attorney Act, 1882
- ▶ A trust as defined in section 3 of the Indian Trusts Act, 1882
- ▶ A will defined in Section 2 (h) of the Indian Success Act, 1925, including any other testamentary disposition by whatever name called
- ▶ Any contract for sale or conveyance of immovable property or any interest in such property
- ▶ Any such class of documents or transactions as may be notified the Central Government in the Official Gazette.

Module 7, Chapter 5

Some of the salient aspects covered under the Act include:

- ▶ The Act defines various terms relating to electronic means of processing, communication, storage and security. Some of these include – electronic form, information, data, computer, computer network, computer system, computer resource, secure system, access, digital signature, private and public key, asymmetric cryptosystem, affixing of a digital signature.
- ▶ Method of authentication of electronic records using digital signature and its verification
- ▶ Legal recognition of electronic records and digital signatures and their use in Government and its agencies
- ▶ Attribution, time and place of despatch and acknowledgment of receipt of electronic records
- ▶ Security procedure for securing electronic records
- ▶ Method of retention of electronic records and their retrieval
- ▶ Empowers the Government to make necessary rules by Central Government, regulation of certifying authorities
- ▶ Enabling the legal administrative structure to support the administration of the Act, including licensing, regulation and audit of certifying authorities, setting up of Cyber Regulations Appellate Tribunal
- ▶ Digital Signature Certificates, their revocation and management and duties of subscribers

The Act also provides for various penalties which include penalties for damage to computer, computer system etc., failure to furnish information, return etc.

The act also specifies the acts that invite penalty of upto Rupees One Crore, which include any:

- ▶ Unauthorised accessing or securing access to such computer, computer system or computer network
- ▶ Unauthorised downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium
- ▶ Introduces or causes to be introduced any computer contaminant of computer virus into any computer, computer system or computer network
- ▶ Damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network
- ▶ Denies or causes the denial of access to any person authorized to access any computer, computer system of computer network by any means

- ▶ Provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of the Act, rules or regulations made thereunder
- ▶ Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network

Besides the Act also provides penalty of failure to furnish any document or return or report to the Controller or the Certifying Authority, failure to maintain books of accounts or records.

The Act also provide for offences that are liable on conviction to imprisonment or fine upto Rupees Lakh or both. Such offences include tampering with computer source documents, hacking with computer system, publishing of Information, which is obscene in electronic form, using digital signature certificates for unlawful or fraudulent purposes.

The UNCITRAL Code

The United Nations Commission on International Trade Law (UNCITRAL Code) is based on the resolution of the General Assembly of the United Nations. The resolution noted that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as “electronic commerce”. Such means of conducting trade involve the use of alternatives to paper based methods of communication and storage of information. With a view to bring in uniformity of the law applicable to alternatives of paper-based methods of communication and storage of information, the resolution recommended that all States should give favourable consideration to the Model Law when they enact or revise their laws.

Some of the objectives of the Model Law include:

- ▶ Offer national legislators, a set of internationally accepted rules on removal of traditional legal obstacles to e-commerce and thus help creating a more secure legal environment.
- ▶ Remedy the disadvantage caused by inadequate legislations at the national level that hinder smooth trade using electronic means of doing business.
- ▶ Enabling or facilitating the use of electronic commerce and providing equal treatment to users of paper-based documentation and to users of computer-based information.

Accordingly the Information Technology Bill, 1999 was also drawn up taking into consideration the UNCITRAL Code.

The UNCITRAL Model Law on Electronic Commerce, as per the general provisions, applies to any kind of information in the form of a data message used in the context of commercial activities. In this regard, be-

Module 7, Chapter 5

sides defining certain terminologies for the purpose of law, contains the following:

- ▶ Legal recognition of data messages, admissibility and evidential weight of data messages
- ▶ Addresses the requirement of message being “in writing” and identification of original
- ▶ Recognises and requires authentication of data messages through specified methods.
- ▶ Requirement relating to retention of data messages
- ▶ Formation and validity of electronic contracts
- ▶ Attribution of data messages, time and date of dispatch, receipt and acknowledgement of receipt
- ▶ Provisions relating to specific areas of electronic commerce

B. Sarbanes - Oxley Act 2002

Sarbanes-Oxley was a reactive legislative measure to the series of corporate failures involving some of the world’s giant corporations such as the Enron, WorldCom. The giant failures brought to light the stark failures of corporate governance and exposed the ineffective disclosure and reporting practices.

Sarbanes Oxley or more popularly known as SOX or Sarbox was formally adopted as the law in 2002 and generally focused on publicly held companies. The legislation seeks to regulate the following:

- ▶ To enhance the requirements as regards quality and transparency of financial reporting and disclosure, and related internal controls.
- ▶ To require that independent accounting firms conducting the assurance assignments shall not have any other consulting or other relationship with the auditee organisation
- ▶ To formally endorse the accounting standards and practices. As a result the Public Companies Accounting and Overseeing Board
- ▶ To increase the corporate responsibility and accountability

The requirements are primarily driven by two sections viz. section 302 and 404 of the SOX, which specifically require public companies to establish, implement and evaluate their internal controls relating to financial reporting, operating integrity and disclosure.

Section 302: Corporate Responsibility for Financial Reports.

The section requires that the CEO and CFO of each issuer shall prepare a statement to accompany the audit report to certify the “appropriateness of the financial statements and disclosures contained in the periodic report, and that those financial statements and disclosures fairly present, in all material respect, the operations and financial condition of the issuer.” A violation of this section must be knowing and intentional to give rise to liability.

Section 404: Management Assessment of Internal Controls.

Requires each annual report of an issuer to contain an “internal control report”, which shall:

- (1) State the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
- (2) Contain an assessment, as of the end of the issuer’s fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Each issuer’s auditor shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this section shall be in accordance with standards for attestation engagements issued or adopted by the Board. An attestation engagement shall not be the subject of a separate engagement.

Internal Control & COSO

Integrated Framework was prepared in response to recommendations of the National Commission on Fraudulent Financial Reporting. Committee of Sponsoring Organizations (COSO) of the Treadway Commission was formed to support implementation of the Treadway Commission’s recommendations and published the completed Internal Control—Integrated Framework. COSO has released for public comment an Enterprise Risk Management (ERM) Framework that details essential components and concepts of enterprise risk management for all organizations, regardless of size. The Framework also identifies the interrelationships between enterprise risk management and internal control. SEC recognizes the COSO Framework.

Criminal Penalties and Protection

The law creates tough penalties for those who destroy records, commit securities fraud and fail to report fraud.

- ▶ **Failure to Maintain Workpapers.** It is now a felony with penalties of up to 10 years to willfully fail to maintain “all audit or review workpapers” for at least five years. The SEC will establish a rule covering the retention of audit records and the Board will issue standards that compel auditors to keep other documentation for seven years.
- ▶ **Document Destruction.** It is a felony with penalties of up to 20 years to destroy documents in a federal or bankruptcy investigation.
- ▶ **Securities Fraud.** Criminal penalties for securities fraud have been increased to 25 years.
- ▶ **Fraud Discovery.** The statute of limitations for the discovery of fraud is extended to two years from the date of discovery and five years after the act. It was previously one year from discovery and three from the act.

Module 7, Chapter 5

- ▶ Other Provisions. Other provisions protect corporate whistleblowers, ban personal loans to executives, and prohibit insider trading during blackout periods

SOX and IT Controls

SOX has brought into focus the requirements as regards operational integrity and effectiveness of internal controls as regards financial reporting and disclosure requirements. With most organisations now critically dependent on Information technology to achieve their information requirements, internal controls to be adequate and effective need to be implemented through Information systems and general controls.

Amendments to Clause 49 of the SEBI Listing Agreement

To fall in line with the global legislative and regulatory developments on Corporate Governance, the recent amendments to Clause 49 of the Listing Agreement (proposed to be effective from December 2005) now include several stringent stipulations requiring assurance as accuracy of financial reporting and regards the design and accuracy of internal controls. Such stipulations cast significant responsibilities on the Board, Audit Committee, CEO and CFO as regards ensuring the adequacy and effectiveness internal controls.

As part of the internal control requirements relating to financial reporting controls, among other risk management provisions, the amendment requires CEO and CFO to certify that the financial statements and the information contained therein “do not contain any untrue statement or material fact or omission and that such statements are not misleading”

The provision also requires the CEO and CFO to:

- ▶ Take responsibility and make themselves accountable for
- ▶ Design of disclosure controls and procedures
- ▶ To state that they have evaluated the effectiveness of the company’s disclosure controls and procedures
- ▶ Requires them to disclose to the company’s auditors/audit committee on all significant deficiencies in design or operation of internal controls relating to financial disclosures.
- ▶ Identify and report to the auditors:
- ▶ any fraud, whether material or not that involves management of employees having significant role in the company’s internal controls
- ▶ Significant changes in internal controls and related factors and corrective action as regards significant deficiencies or material weaknesses

The amendments to clause 49 of the listing agreement, now make corporate executives take explicit responsibility for establishing a system of internal controls over financial reporting and evaluating and monitoring the effectiveness of such internal controls. With most organisations entirely or significantly dependent on Information Technology, whether

using ERPs or other operational and financial software applications to achieving collation of financial information and financial reporting, controls over IT have become an inherent part of internal control requirement. This creates a challenge in terms of accountability of the IT with regard to quality and integrity of financial information generated using Information technology. The risks of internal controls relating to financial reporting coupled with the inherent risks of using information technology presents with serious control requirements not only in terms of application controls but also in terms of IT general controls, which concerns the control requirements of both management as well as auditors. Hence as part of internal controls requirements, many concerns and requirements and responsibilities arise in terms of IT control requirements, some of these include:

- ▶ Understanding the internal controls relating to financial reporting from a IT perspective
- ▶ Identification of risks arising from use of IT for financial reporting depending on the complexity and nature of such implementations
- ▶ Identification of software applications and other technology components that deliver to financial reporting objectives, whether directly or indirectly
- ▶ Evaluation of internal control framework with regard to design of IT controls, risk management and monitoring
- ▶ Evaluation of adequacy and efficacy of internal controls and related IT controls

C. Basel II Framework for Risk Management

A significant global development that is set to critically impact the Banking Sector is the revision of the framework of standards for establishing minimum capital requirements for banking organisation or more commonly referred to as the Basel II Framework, prepared by the Basel Committee on Banking Supervision.

Basel II seeks to further regulate the minimum capital requirements for banks, which serves as the foundation for a bank's future business and a fall back in case of unexpected losses. What is minimum capital for a bank is often a highly dicey and technical issue, which is determined by a score of factors.

A revision to the earlier Basel Framework was necessitated by the significant advances in banking industry worldwide and the much needed changes in risk management practices, use of technology and changing banking markets.

Good risk management and supervision practices are a key component of the success of a banking organisation. Realising the need for appropriate and sophisticated risk management practices, the Basel II provides for the state of such practices being reflected in the capital regulations.

Module 7, Chapter 5

This promotes and encourages improved risk management practices further strengthening the stability of the financial system.

As against the single financial oriental basis provided by earlier Basel Accord, Basel II has introduced 3 pillars, each complementing and supplementing the others and enable banks to enhance the quality of their internal processes. Such pillars focus on minimum capital requirements, supervisory review and market discipline. It is also essential, as part of the bank's management process, to provide for adequate capital to protect against overall risks, which to a significant extent includes operational risks. Such risks are based on internal risk assessments, based on risk profiles set up by each bank, need to develop adequate and sound control structures and continually improve processes. Further the banks need to set an example through prudent management and enhancing the degree of transparency in public reporting of the banks through greater disclosures and adequacy of capital set aside.

Operational risks are risks that result from inadequate or failed internal processes, people and systems or from external events. Hence operational risks need to be measured and managed, to trigger suitable supervisory actions. Significant amounts of data on various internal and external risks and related controls is significant. Such data includes both internal and external data, data relating to internal controls and business environment, scenario analysis. Hence there is need for extensive data and analysis relating to operational risk corporate governance, operational risk losses, risk quantification and mitigation.

In every economy, generally, banks have been leading the automation of business processes with the extensive use of Information Technology. Banks have more than been an enabler for banking organisation with newer innovations and products such as the internet banking and anywhere/anytime banking etc. The various banking application software now embed or are believed embed the required internal controls, which are a key risk mitigation factors for this industry. This has also introduced the need for real-time monitoring to enhance database security, availability and integrity.

Adequate controls need to be in place to ensure that all transactions are captured, processed and recorded safely, accurately and confidentiality. The newer risks arising from constantly updating web based development products and modules need to be continually monitored for newer areas of operational risks. Suitable systems for identification, capture, storage, analysis, retrieval and dynamic reporting of data relating to operational risk.

Summary

The legal and regulatory environment in which it operates, directly affects every enterprise that pursues its business objectives. The IS auditor, before commencing his audit should be aware of the various governmental and external requirements that impact the controls and practices relating to Information Technology and related controls. The auditor should also be aware of the IS audit standards, guidelines and procedures relating to the attitude and performance of audit work. Standards and best practices such as BS7799, COBIT, ITIL and SAS 70 are amongst the globally recognized benchmarks for evaluating an organisations's capability and status as regards various facets of Information Security and IT Governance.



Questions

1. The most common reason for IS exposures is due to:
 - A. Errors, negligence and low-tech manipulations by insiders
 - B. Hacking
 - C. Computer Equipment breakdown
 - D. Natural disasters such as fire, earthquake and floods
2. IS security is not concerned with:
 - A. Possibilities of fraud and error
 - B. Ability to manage IT resources effectively
 - C. Attempt of company to keep its information intact
 - D. Ability to recover from disasters like data loss with minimum damage
3. The objective of IS security is least likely to include:
 - A. Strategy for risk management
 - B. Procedures and practices to assure that computer facilities are available at all required times
 - C. Complete and efficient processing of data occurs
 - D. Restriction of data access to authorized users
4. The risk assessment process involves all of the following except:
 - A. Take steps to reduce risk to an acceptable level
 - B. Assess probability of occurrence of threats
 - C. Identify the IT resources
 - D. Ascertain the risk profile
5. The risk assessment approach should ensure that formal agreement on residual risk. The most critical factor on which this depends is:
 - A. Risk identification and measurement

Module 7, Questions

- B. Corporate policy
 - C. Adopting risk assessment approach of that of the competitor
 - D. Cost effectiveness of implementing safeguards and controls
6. Exposures refer to:
- A. Quantification of potential impact of problem
 - B. Causes of risk
 - C. Audit objectives
 - D. Alignment of functions
7. Changes in traditional controls in a computerized environment is least likely to impact:
- A. Transfer of responsibilities
 - B. Decline in accountability
 - C. Audit objectives
 - D. Alignment of functions
8. The most critical control consideration in designing the audit procedures in a computerized environment is:
- A. Lack of segregation of duties
 - B. Lack of management control
 - C. Lack of IT knowledge by IT staff operating the system
 - D. The online and real time nature of the system
9. The most important factor to be considered in case of an IT environment is:
- A. Inherent risks
 - B. Physical access control impact IT
 - C. Environmental controls impact IT
 - D. CAATs are used for audit
10. The key objective of control is to:
- A. Implement appropriate policy, procedures and practices
 - B. Establish appropriate organisation structure
 - C. Provide reasonable assurance that business objectives are achieved
 - D. Facilitate management of information systems
11. The objective of the audit mission statement is to:
- A. Outline the purpose and value addition of the audit function
 - B. Lay down the priority for the areas of audit
 - C. Outline the responsibility, authority and responsibility of the IS Audit function
 - D. Assess the competency and skill requirements of the IS Audit function
12. The objective of an audit charter is to:
- A. Serve as a control framework for outsourced audit engagements

Module 7, Questions

- B. Outline the responsibility, authority and responsibility of the IS Audit function
 - C. Prescribe the audit program and procedures
 - D. A top level document that defines the rights, authority and responsibilities of the management towards the audit function
13. Which of the following forms of evidence would be considered to be the MOST reliable?
- A. An oral statement from the auditee
 - B. The results of a test performed by an IS auditor
 - C. An internally generated computer accounting report
 - D. A confirmation letter received from an outside source
14. IS audit refers to any audit that encompasses review and evaluation of:
- A. Efficiency of computing resources and networking technologies
 - B. Controls in Computerised information systems
 - C. Risks and controls as regards use of IT for business
 - D. Automated information processing systems and its interfaces
15. Skills and competence requirements of an IS Auditor must include:
- A. Proficient programming skills
 - B. Sound knowledge of business operations, practices and compliance requirements and related IT risks and controls
 - C. A general understanding of systems design and project management concepts
 - D. In-depth knowledge of risks and controls relating to various Information technologies
16. The scope and objective of an IS audit assignment is:
- A. Always specified by regulation
 - B. Determined by the IS auditor
 - C. Specified by the user management
 - D. Agreed in discussion with the senior management
17. An IS Auditor appointed to conduct an IS audit of networking controls is expected to perform all of the following except:
- A. Identify and evaluate control weaknesses
 - B. Provide report on the findings and recommendations
 - C. Follow up implementation of recommendations
 - D. Ensure that controls are effectively installed by participating in implementing the controls

Module 7, Questions

18. An audit firm is offered the engagement to conduct a Network security audit of the ATM systems of a large national bank. In such a situation, the audit firm should:
- A. Accept the audit even though internal competencies may not be available
 - B. Not accept the assignment since it does not possess the competencies
 - C. First evaluate the audit risk of conducting the audit with available internal competencies and explore the options of relying on the services of an expert
 - D. Accept the audit first and take immediate steps to gain the knowledge and competence through intensive training.
19. An important distinction an IS auditor should make when evaluating and classifying controls as preventive, detective or corrective is:
- A. the point when controls are exercised as data flows through the system.
 - B. only preventive and detective controls are relevant.
 - C. corrective controls can only be regarded as compensating.
 - D. classification allows an IS auditor to determine which controls are missing..
20. An IS auditors is expected to use due professional care when performing audits, which requires that the individual exercise skill or judgment:
- A. Commonly possessed by practitioners of that specialty.
 - B. Which includes programming skills in the software under review.
 - C. Relating to the selection of audit tests and evaluation of test results.
 - D. Where an incorrect conclusion based on available facts will not be drawn..
21. An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor perform FIRST?
- A. Personally delete all copies of the unauthorized software.
 - B. Inform auditee of the unauthorized software and follow-up to confirm deletion.
 - C. Report the use of the unauthorized software to auditee management and the need to prevent recurrence.
 - D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Module 7, Questions

22. An IS Auditor has been assigned the task of reviewing the Information Systems Security of a Sales Database, this refers to evaluation of Information based on the following criteria:
- A. Effectiveness, Efficiency and Authenticity
 - B. Confidentiality, Integrity and Availability
 - C. Availability, Integrity and Reliability
 - D. Confidentiality, Compliance and Reliability
23. The document least likely to be considered in an Application Controls audit is:
- A. User manual
 - B. Business process rules
 - C. Work flow procedures
 - D. Coding standards
24. The audit procedure which could be common to auditing Information Security as well as for a financial audit and for IS audit is:
- A. Review technical documentation
 - B. Inspection
 - C. Use CAATs for finding open ports
 - D. Review of Information Security Policy
25. Which of the following is an anti-virus detective control?
- A. Route all links to external systems via a firewall.
 - B. Scan all diskettes and CDs brought in from outside the company before use.
 - C. Scan all files on all file server hard disks daily, moving suspect files to a safe area.
 - D. Use anti-virus software to update users' anti-virus configuration files every time they log in
26. The risk that an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when, in fact, they do, is an example of:
- A. inherent risk.
 - B. control risk.
 - C. detection risk.
 - D. audit risk.
27. During a review of the controls over the process of defining IT service levels an IS auditor would MOST likely interview the:
- A. Business unit manager.
 - B. Legal staff.
 - C. Systems programmer.
 - D. Programmer.

Module 7, Questions

28. The most critical impact on an internal control system on account of computerization is:
- A. High volume of processing of transactions
 - B. Extent of substantive procedures could be reduced
 - C. Internal control systems get in-built into the applications
 - D. Inherent risks of information technology as deployed
29. Compliance testing could be most effectively used for testing the:
- A. Completeness of transactions
 - B. Accuracy of transactions
 - C. Implementation of controls as per policy
 - D. Processing of transactions
30. Which of the following is a detective control?
- A. Physical access controls
 - B. Segregation of duties
 - C. Back-up procedures
 - D. Audit trails
31. IS auditors, auditing through computers are not expected to:
- A. Be aware of the fundamental concepts of Information Technology
 - B. Know the key components of IT and how they function
 - C. Be experts in technology behind development of CAATs
 - D. Understand business process controls
32. The most effective option of using computer programs for testing client data is:
- A. Use the client's program
 - B. Write a program specifically for the purposes of the audit
 - C. Use a generalized audit software
 - D. Use a walk-through approach to understanding the process
33. Using Generalised Audit Software for testing application if correct rates are applied to sales invoices involves:
- A. Testing the logic and sales data of the auditee
 - B. Testing the actual sales data from the database of the client organisation
 - C. Testing the auditee's sales application software
 - D. Testing the access controls
34. The first step to using an audit software is to:
- A. Collect the test data
 - B. Understand the test objectives
 - C. Evaluate the test results
 - D. Identify IT resources required for the testing

Module 7, Questions

35. An auditor plans to use CAATs extensively for conducting an internal audit of manufacturing operations of an enterprise. CAATs are least likely to be used for:
- A. Drawing out appropriate samples
 - B. Interface with production databases to query
 - C. Report the audit findings with evidence
 - D. Uncover fraudulent transactions
36. With regard to an external audit agency entrusted with review of controls in sales and inventory processes in a computerized information systems environment, the audit approach will significantly differ with regard to:
- A. the method of fixation of audit objectives and scope
 - B. the procedures followed by the auditor in obtaining a sufficient understanding of the accounting and internal control system.
 - C. the methods for rating of risks based on his findings
 - D. the degree of performance of compliance and substantive test procedures in a computerized environment as compared to a non-computerised environment
37. An auditor would use the black box approach:
- A. To test for suspected transactions or suspected practices
 - B. In case the audit does not involve testing controls in a computerized information systems environment
 - C. To evaluate the controls in computerized systems by analyzing the outputs from a computerised system against calculated results for a given set of inputs
 - D. To map the logic path and controls in the application software.
38. Entrusted with the objective of identifying errors or deviations in the controls relating to inventory application software, which of the following would the auditor find most appropriate for the purpose:
- A. Black box approach
 - B. Snapshot technique
 - C. Integrated test facility
 - D. Waterfall model
39. The risks of using the integrated test facility is:
- A. The controls in application may not be tested
 - B. The processing of data may not be tested
 - C. The effects of testing using test data may adversely impact the integrity of the production database
 - D. The modifications for audit testing made to application in live environment may not be removed entirely.
40. The most critical risk in embedded audit facility is:
- A. Specially designed modules are not appropriately embedded in the application

Module 7, Questions

- B. Selected data is stored on the auditee's computer
 - C. Selected data can be modified by the auditee's management
 - D. Data collection modules are inserted in the application at points determined by the auditee management.
41. IS audit standards:
- A. Specify the manner in which an IS audit should be carried out
 - B. Provide recommendations on improvement of audit performance
 - C. Provide auditors with a clear idea of the minimum level of acceptable performance
 - D. Provide guidance to professionals on audit on performing IS audit in specified environments
42. CIS under AAS 29 of ICAI refers to:
- A. Continuous and systematic information
 - B. Continuous and Intermittent Simulation
 - C. Computerised Information Systems
 - D. Computerised Information Sources
43. COBIT is:
- A. A standard to be followed by IS auditors while conducting IS Audit
 - B. A comprehensive standard for IT Governance
 - C. A multi-purpose audit tool for testing application controls
 - D. A standard for Corporate Governance
44. An organisation seeks to get its Information Security Management Systems certified by an independent certifying agency, which of the following standards would be useful in this regard:
- A. COBIT
 - B. SAS 70
 - C. BS7799
 - D. ITIL
45. IT Infrastructure Library (ITIL) deals with:
- A. Information Technology controls for organisations requiring secure implementation
 - B. Best practices for quality of IT services and its management
 - C. A governance model for management of IT
 - D. Internal controls in Information Technology for integrity of financial reporting
46. The Information Technology Act:
- A. Defines the method of authentication of an electronic record
 - B. Provides for authentication of all electronic records using digital signature
 - C. Encourages the use of digital signatures for all government

- transactions
- D. Requires the use of electronic signatures using symmetric cryptography
47. The Information Technology Act does not apply to all of the following, except:
- A. A e-banking mechanism used instead of a cheque
 - B. A will
 - C. Electronic contract for sale of building
 - D. Notification of documents in the Government Gazette through electronic means
48. Which of the following is a not an offence under the Information Technology Act, 2000:
- A. Introducing a virus into the network of an organisation
 - B. Providing assistance to any person to facilitate unauthorized access to any computer system
 - C. Creating a software to cause denial of service attack
 - D. Damaging the computer system by changing an operating system parameter with a view to cause disruption to business
49. Sarbanes-Oxley Act 2002 seeks to regulate:
- A. Control requirements relating to Information Technology governance and controls, especially those relating to financial disclosure controls
 - B. To enhance requirements as regards quality and transparency of financial reporting and disclosure and related internal controls and corporate responsibility thereof
 - C. To empower audit committees
 - D. To check the rate of growing computer crime
50. Which of the following would qualify to be a requirement under the IT Act, 2000:
- A. Requiring signatures on all documents generated
 - B. Controls over time and date stamping of data messages
 - C. Controls over physical security of computer equipment
 - D. Use of standard software for firewalls

Answers

QUESTION No	1	2	3	4	5	6	7	8	9	10
ANSWERS	A	B	B	A	D	A	C	A	A	C

QUESTION No	11	12	13	14	15	16	17	18	19	20
ANSWERS	A	B	D	D	B	D	D	C	A	A

Module 7, Questions

QUESTION No	21	22	23	24	25	26	27	28	29	30
ANSWERS	C	B	D	B	C	C	A	C	C	D

QUESTION No	31	32	33	34	35	36	37	38	39	40
ANSWERS	C	C	A	B	C	D	C	B	C	A

QUESTION No	41	42	43	44	45	46	47	48	49	50
ANSWERS	C	C	B	C	B	A	D	C	B	B

References

Stepping through IS Audit, J. L. Bayuk, ISACA

Managing the Information Systems audit, Billy Smith, IIA

Core concepts of IT Auditing, James E. Hunton, Stephanie M. Bryant, Nancy A. Bagranoff, John Wiley & Sons

Information Technology Control and Audit, 2nd Edition, Fredrick Gallegos, Daniel P.Manson, Sandra Senft, Carol Gonzales, Auerbach,USA, 2004



Glossary

- Abstraction** ➤ This refers to the property in Object-Oriented Systems where only the essential and inherent aspects are focussed and other aspects are ignored.
- Accelerator** ➤ A hardware addition to an existing computing device that increases the computer's processing speed and capabilities.
- Access** ➤ Referring to the ability of a computing device to use data or resources beyond its native capabilities.
- Access Control** ➤ A technique used to permit or deny use of data or information system resources to specific users, programs, processes, or other systems based on previously granted authorization to those resources.
- Access Control List (ACL)** ➤ List that specifies who can do what with an object. For example, an ACL on a file specifies who can read, write, execute, delete, or otherwise manipulate the file.
- Access List** ➤ A list kept by routers to control access to or from the router for a number of services. For example, the list can prevent packets with a certain IP address from leaving a particular interface on the router.
- Access Method** ➤ The type of Media Access Control method that a node uses to gain control of a network.
- Access Point** ➤ A layer two connectivity device that interfaces wired and wireless networks and controls the networking parameters of its wireless LAN.
- Account Expiration** ➤ A date after which an account cannot be used.
- Account Lockout** ➤ A method of disabling an account after some number of incorrect tries at logging on is unsuccessful. This control is usually set in order to automatically disable accounts that are being brute-forced. See also Brute-Force Attack.
- Accountability** ➤ The ability to trace activities on information resources to unique individuals who accept responsibility for their activities on the network.
- Acknowledgment** ➤ Notification sent from one network device to another to acknowledge that some event (for example, receipt of a message) has occurred. Sometimes abbreviated ACK.

Glossary

- Activation** ➤ Process of putting into motion the whole or portion of a recovery plan.
- Active Hub** ➤ Multi-ported device that amplifies LAN transmission signals.
- Active Monitor** ➤ Device responsible for managing a Token Ring. A network node is selected to be the active monitor if it has the highest MAC address on the ring. The active monitor is responsible for management tasks such as ensuring that tokens are not lost or that frames do not circulate indefinitely.
- Active Scanning** ➤ A method by which client devices discover wireless networks. Active scanning involves a client device broadcasting a probe request frame and receiving a probe response frame containing the parameters of the responding network.
- Ad-hoc Network** ➤ A wireless LAN composed of wireless stations without an access point. Also referred to as an independent network or Independent Basic Service Set (IBSS).
- Adapter** ➤ Hardware that allows a computing device physical access to a network.
- Address Mapping** ➤ Technique that allows different protocols to interoperate by translating addresses from one format to another. For example, when routing IP over X.25, the IP addresses must be mapped to the X.25 addresses so that the IP packets can be transmitted by the X.25 network. See also Address Resolution.
- Address Mask** ➤ Bit combination used to describe which portion of an address refers to the network or subnet and which part refers to the host. Sometimes referred to simply as Mask.
- Address Resolution** ➤ When two addressing systems refer to the same entity, the process of translating or expressing the address of an entity on one system to the equivalent address of the same entity in the second system. For instance, translating an IP address to its given DNS name.
- Administrative Controls** ➤ The plan of organization and procedures that are concerned with the decision process leading to management authorization of transactions
- AIX** ➤ IBM's implementation of Unix.
- Alert** ➤ Either (noun) a high-priority threat event communicated in real time, or (verb) to bring attention to a security violation or activities that exceed predefined thresholds, in an immediate manner so as to provoke immediate response.

- Algorithm** ➤ A set of rules and decision structures for actions in a specifically defined set of circumstances.
- Alphanumeric** ➤ Referring to a group of printable characters that includes the letters of the alphabet in both upper and lower case, the numerals plus a limited group of additional symbols and punctuation marks.
- Alternate Site** ➤ Location, other than the main facility, that can be used to conduct business functions. Similar Terms: Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility.
- Amplitude** ➤ In the terminology of wave motion, the height of the wave. Amplitude is usually measured from a reference point of 0. In electrical waves, amplitude is typically expressed in volts.
- Analog Transmission** ➤ Signal transmission over wires or through the air in which information is conveyed through variation of some combination of signal amplitude, frequency, and phase.
- Anomaly Detection (AD)** ➤ An IDS model that detects threats by modeling known good network behavior and characteristics and alerting on exceptional differences. See also Intrusion Detection System.
- ANSI (American National Standards Institute)** ➤ The principal group in the US for defining standards.
- API (Application Programming Interface)** ➤ A set of tools and procedures provided by the programmer of an application so that other programmers can control, exchange data with, or extend the functionality of an application.
- Appending Virus** ➤ A computer virus that inserts itself at the end of a host file. See also Boot Virus, Macro Virus, Memory-Resident Virus, Multipartite Virus, Nonresident Virus, Overwriting Virus, Parasitic Virus, Prepending Virus, Stealth Virus, and Virus.
- Application** ➤ An independently executable set of algorithms and data structures that perform a specific set of functions.
- Application Controls** ➤ Programmatic and manual procedures used to verify the correctness and accuracy of application processing
- Application Layer** ➤ Layer 7 of the OSI reference model. This layer provides services to application processes (such as electronic mail, file transfer, and terminal emulation) that are outside of the OSI model. The application layer identifies and establishes the availability of intended communication partners (and the resources required to connect with them), synchronizes cooperating applications, and agreement on procedures for error recovery and control of data integrity. See also

Glossary

Data Link Layer, Network Layer, Physical Layer, Presentation Layer, Session Layer, and Transport Layer.

Application Program ➤ Processes the business data by data entry, update or query.

Application Recovery ➤ The component of Disaster Recovery which deals specifically with the restoration of business system software and data, after the processing platform has been restored or replaced. Similar Terms: Business System Recovery.

Application Software ➤ Software developed or bought out and employed for automating business operations and activities, e.g. payroll, sales, inventory, ERP etc.

Application System ➤ An integrated set of computer programs designed to serve a particular function that has specific input, processing and output activities (e.g., general ledger, manufacturing resource planning, human resource management).

Architecture ➤ The sum total of all of the specifications, protocols and implementations that define a particular networking system.

Archive ➤ A storage of infrequently-used or historical data.

ARPA (Advanced Research Projects Agency) ➤ Research and development organization that is part of US Department of Defense. ARPA is responsible for numerous technological advances in communications and networking. ARPA evolved in DARPA, and then back into ARPA again (in 1994). See also DARPA.

Arpanet (Advanced Research Projects Agency Network) ➤ Landmark packet-switching network established in 1969 by BBN and funded by ARPA (and later DARPA). It eventually evolved into the Internet. The term ARPANET was officially retired in 1990.

Artificial Intelligence ➤ The computer systems which can simulate the human intelligence using a pre determined set of rules.

ASCII (American Standard Code For Information Interchange) ➤ Referring to a standard 7-bit character system that includes the alphanumeric characters and printer control codes.

Assembler ➤ A translator that takes an assembly level code as input and produces corresponding machine code as output.

Asynchronous ➤ A system of communication in which each discreet delivery of information establishes its own timing impulse rather than having to conform to the timing impulse of previous deliveries.

- Asynchronous Transmissions** ➤ Term describing digital signals that are transmitted without precise clocking. Such signals generally have different frequencies and phase relationships. Asynchronous transmissions usually encapsulate individual characters in control bits (called start and stop bits) that designate the beginning and end of each character. Compare with Synchronous Transmission.
- AT Commands** ➤ A set of commands that control a modem or alter its characteristics.
- ATDM** ➤ Asynchronous Time Division Multiplexing. Method of sending information that resembles normal TDM, except that time slots are allocated as needed rather than pre-assigned to specific transmitters. Compare with FDM, Statistical Multiplexing and TDM.
- ATM** ➤ Asynchronous Transfer Mode. A broadband transmission system using 53-octet packets over a cell-switched network at speeds up to 2.2 GBPS.
- Attack** ➤ Unauthorized activity with malicious intent that uses specially crafted code or techniques.
- Attack Scripts** ➤ Prepackaged collections of hostile software that are intended to be easy to use and don't necessarily require any special skills or knowledge on the part of the user. Attack scripts can be used by anybody who wants to attack computer systems and networks.
- Attack Signature** ➤ The characteristics of network traffic, either in the heading of a packet or in the pattern of a group of packets, which distinguish attacks from legitimate traffic.
- Attacker** ➤ A person or computer program that intentionally attempts to gain unauthorized access to information resources, or that attempts to prevent legitimate access to those resources.
- Attenuation** ➤ A loss in the amplitude or strength of a signal due to an interaction with the signal's media. Generally expressed in decibels.
- Attribute** ➤ Configuration data that defines the characteristics of database objects such as the chassis, cards, ports, or virtual circuits of a particular device. Attributes might be preset or user-configurable. On a LightStream 2020 ATM switch, attributes are set using the configuration program or CLI commands.
- Audit** ➤ An independent review and examination of records and observation of activities to check that security controls comply with established security policies and procedures, and to recommend any necessary changes in those controls, policies, and procedures.

Glossary

- Audit Trail** ➤ A chronological record of activities on information resources that enables the reconstruction and examination of sequences of activities on those information resources for later review.
- Authentication** ➤ Verification of who a person or information resource claims to be that sufficiently convinces the authenticator that the identity claim is true. This is followed by an evaluation of whether that entity should be granted access to resources.
- Authorization** ➤ A determination, based on prior authentication, of what rights a person or information resource has, and what elements they should be granted access to.
- Authorized** ➤ Having been granted access, based on appropriate authentication and authorization rules and security checks.
- Availability** ➤ Requirement for information to be accessible as and when required and in the manner required. This objective protects against intentional or accidental attempts to deny legitimate users access to information and/or systems
- Back Door** ➤ A means of bypassing established authentication, authorization, and access controls protecting an information resource. Back doors are usually left in place intentionally by the original developers to allow them unauthorized access by circumventing security controls. Also called a Trap Door.
- Back End** ➤ Node or software program that provides services to a front end. See also client, front end, and server.
- Back End Processor** ➤ A computer running an application that supplies data to other computers on demand, but has no user interface.
- Backbone** ➤ Referring to the internet, a central network that provides a pathway for other networks to communicate.
- Background Task** ➤ A computing task that is executing while another task or application is displaying its user interface.
- Backup** ➤ A copy of a set of files made for replacement purposes in case the original set is damaged or lost.
- Backup Strategies (Recovery Strategies)** ➤ Alternative operating method (i.e., platform, location, etc.) for facilities and system operations in the event of a disaster.
- Backward Compatible** ➤ An upgraded component of a computing system that can be used interchangeably with its previous version.
- Backward Learning Algorithm** ➤ Process used for routing traffic that surmises information by assuming symmetrical network conditions. For

example, if node A receives a packet from node B through intermediate node C, the backward-learning routing algorithm will assume that A can optimally reach B through C.

Bandwidth ➤ In analog communications, the difference between the highest and lowest frequencies available in the band. In digital communications, bandwidth is loosely used to refer to the information-carrying capacity of a network or component of a network.

Baseband ➤ A communication system in which only one signal is carried at any one time.

Batch Processing System ➤ A system where transactions are collected over a period of time and processed in one stroke.

Baud ➤ Unit of signaling speed equal to the number of discrete signal elements transmitted per second. Baud is synonymous with bits per second (bps), if each signal element represents exactly 1 bit.

Bind ➤ Berkeley Internet Name Domain. The standard TCP/IP naming service that links network names with IP addresses.

Bit Rate ➤ The rate at which bits are transmitted or received during communication, expressed as the number bits in a given amount of time, usually one second.

Bitmap ➤ A data structure that uses bits to represent the attributes of an object that is not character-based.

Black Box ➤ A device that performs a function using mechanisms that are unimportant or impossible to understand.

Black Box Approach ➤ An auditing approach that does not expect the IS Auditor to have knowledge of the internals of the system. The approach involves comparing the output generated from the computer with pre-computed results for a given set of inputs.

Black Box Testing ➤ The testing which involves the testing of the functionality of the software which does not require the knowledge of the coding.

Blocking Access ➤ Protecting a network or system by keeping unauthorized parties out using an all-or-nothing paradigm instead of using a granular or graduated approach.

BNC ➤ Bayonet "N" Connector. 1. The locking connector type used in 10Base2 (Thin Ethernet). 2. Any connector similar to the type used by 10Base2 for CATV, and other electronic uses.

Boot ➤ Startup operation of a computer.

Boot Drive ➤ The disk that contains a computer's startup instructions.

Glossary

- Boot Virus** ➤ A computer virus that infects a hard drive or floppy disk boot sector. See also Appending Virus, Macro Virus, Memory-Resident Virus, Multipartite Virus, Nonresident Virus, Overwriting Virus, Parasitic Virus, Prepending Virus, Stealth Virus, and Virus.
- BRI(Basic Rate Interface)** ➤ An ISDN service with two bearer channels at 64 KBPS plus a “Data-Link” or control channel at 16 KBPS.
- Bridge** ➤ A Data Link Layer device that limits traffic between two network segments by filtering the data between them based on hardware addresses.
- Broadband** ➤ A transmission system capable of carrying many channels of communication simultaneously by modulating them on one of several carrier frequencies.
- Broadcast** ➤ An information transmission that is intended to be interpreted by all entities capable of receiving it. See also Unicast
- Router** ➤ A device that incorporates the functionality of a bridge and a router in a single unit.
- Brute-Force Attack** ➤ A method used for breaking encryption systems. Brute-force methodology entails trying all the possible keys until the proper one is found.
- Buffer** ➤ A temporary memory storage area for information.
- Buffer Overrun** ➤ Copying too much information to a memory location, leading to denial of service or elevation of privilege attacks.
- Bug** ➤ A flaw in a software program.
- Bus Topology** ➤ Linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Compare with Ring Topology, Star Topology, and Tree Topology.
- Business Continuity Planning (BCP)** ➤ Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue without interruption or essential change.
- Business Impact Analysis (BIA)** ➤ Process of determining the impact on an organization, should a potential loss identified by the risk analysis actually occur. The BIA should quantify, where possible, the loss impact from both a business interruption (number of days) and a financial standpoint.

- Business Interruption** ➤ Any event, whether anticipated (such as public service strike) or unanticipated (such as blackout) which disrupts the normal course of business operations at a corporate location.
- Business Interruption Costs** ➤ The costs or lost revenue associated with an interruption in normal business operations.
- Business Recovery Process** ➤ The common critical path that all companies follow during a recovery effort.
- Cache** ➤ A group of memory locations set aside for temporary storage of data, especially frequently-used data or data needing high speed retrieval by the CPU.
- Case-Insensitive** ➤ Referring to a system in which upper case letters are not differentiated from their lower case form.
- Case-Sensitive** ➤ Referring to a system in which upper case letters are differentiated from their lower case form.
- Cell** ➤ The basic unit for ATM Switching and multiplexing. Cells contain identifiers that specify the data stream to which they belong. Each cell consists of a 5-byte header and 48 bytes of payload. See also Cell Relay.
- Challenge and Response** ➤ An authentication process whereby the server sends a challenge message to the client, and the client responds, usually by encrypting the challenge with the client's password hash and then returning the result as the response.
- Change Control** ➤ A formal procedure that is used to approve and manage all modifications to software and hardware.
- Channel** ➤ A communication path.
- CHAP (Challenge Handshake Authentication Protocol)** ➤ Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, it merely identifies the remote end. The router or access server then determines whether that user is allowed access. Compare with PAP.
- Cheapernet** ➤ Industry term used to refer to the IEEE 802.3 10Base2 standard or the cable specified in that standard. Compare with Thinnet. See also 10Base2, Ethernet, and IEEE 802.3.
- Checklist Test** ➤ A method used to test a completed disaster recovery plan. This test is used to determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.
- Checksum** ➤ The result of a mathematical operation that uses the binary representation of a group of data as its basis, usually to check the integrity of the data.

Glossary

Cipher ➤ An encoded message.

CIS ➤ Expands to Computerised Information Systems - CIS environment exists when one or more computer(s) of any type or size is (are) involved in the processing of financial information, including quantitative data, of significance to the audit, whether those computers are operated by the entity or by a third party.

Class ➤ In Object Oriented technology, classes are used to distinguish one type of object from another and is a generic form of an object.

Client ➤ Node or software program (front-end device) that requests services from a server. See also Back End, Front End and Server.

Client/Server ➤ A type of relationship between two computers where the two have different roles in the relationship. Typically, the client computer drives the relationship and uses a resource of the server computer.

Client-Side Script ➤ A programming script, written in a scripting language such as JavaScript or VBScript, that is invoked at the endpoint system rather than on the central server.

Cluster Controller ➤ 1. Generally, an intelligent device that provides the connections for a cluster of terminals to be data link.

Coaxial Cable ➤ An electrical cable in which the conductors share a common axis.

COBIT (Control Objectives For Information And Related Technology) ➤ The international set of IT control objectives published by ISACF and IT Governance Institute

Cold Site ➤ Alternate operating facility that is void of any resources or equipment except air-conditioning and electrical wiring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Similar Terms: Shell-Site.

Collision ➤ In Ethernet, the result of two nodes transmitting simultaneously. The frames from each device are damaged when they meet on the physical media. See also Collision Domain.

Collision Avoidance ➤ A Media Access Control (MAC) method in which any node may take control of the network after taking certain steps to ensure that the cable is not in use or about to be used by another node.

Collision Detection ➤ A MAC method in which any node may take control of the network when it is not in use by another node. While transmitting, stations continue to listen for incoming signals (collisions) and emit a jamming signal to notify all other stations of the collision.

- Common Carrier** ➤ Licensed, private utility company that supplies communication services to the public at regulated prices.
- Communication Server** ➤ Communications processor that connects asynchronous devices to a LAN or WAN through network and terminal emulation software. Performs only asynchronous routing of IP and IPX. Compare with Access Server.
- Communications Failure** ➤ An unplanned interruption in electronic communication between a terminal and a computer processor, or between processors, as a result of a failure of any of the hardware, software, or telecommunications components comprising the link.
- Communications Recovery** ➤ The component of Disaster Recovery which deals with the restoration or rerouting of an organization's telecommunication network, or its components, in the event of loss. Similar Terms: Telecommunication Recovery; Data Communications Recovery.
- Comparison Program** ➤ A program which can be used for the examination of the data using the logical or conditional tests to determine similarities or differences.
- Compiler** ➤ A translator that takes a program source code as an input and produces corresponding machine code as output. A compiler takes a program as a single unit, compiles the same, checks for errors and if error-free, produces machine code as the output. Every programming language, has its own compiler(s).
- Computer** ➤ A computer is an interrelated combination of components that performs the function of input, processing, output, storage and control, thus providing end users with powerful data processing capability.
- Computer Aided Software Engineering (CASE)** ➤ A software which helps in the development of all phases of the information system. This software is an automation aid for system analysis, design programming and documentation.
- Concentrator** ➤ A synonym for a multi-port repeater that may also perform bridging and routing functions.
- Conductor** ➤ The current-carrying component of a transmission cable, typically a copper wire.
- Confidential Information** ➤ Information that requires special handling and protection because it is not intended to be viewed, modified, or discarded by everyone.
- Confidentiality** ➤ The characteristic of data and information being disclosed only to authorized persons, entities, and processes at authorized times

Glossary

and in an authorized manner. Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.

Configuration Management ➤ One of five categories of network management of OSI networks. Configuration management subsystems are responsible for detecting and determining the state of a network. See also Account Management, Fault Management, Performance Management, and Security Management.

Congestion ➤ Traffic in excess of network capacity.

Connectionless ➤ Describes network protocols that do not establish a connection between the source and destination before transmitting data. Compare with Connection-Oriented. See also Virtual Circuit.

Connection-Oriented ➤ Describes network protocols that establish and confirm a connection between source and destination hosts before transmitting data.

Consortium Agreement ➤ An agreement made by a group of organizations to share processing facilities and / or office facilities, if one member of the group suffers a disaster. Similar Terms: Reciprocal Agreement.

Containment Fields ➤ Areas of a network (or different networks) that are separated with the use of access control technologies, such as firewalls and access control lists (ACLs), because those areas of the network have security requirements that differ from each other. See also Access Control List.

Contingency Planning ➤ Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.

Controls ➤ Measures designed to reduce or deter threats.

Cooperative Hot-Sites ➤ A hot site owned by a group of organizations available to any group member, should a disaster strike.

Correlation ➤ Organizing and recognizing one related event threat out of several reported, but previously distinct, events.

Cracker ➤ A hacker who attempts to break into computers. See also Hacker.

CRC (Cyclic Redundancy Check) ➤ A method of ensuring data integrity where a calculation is performed using the binary representation of the data itself as the basis of the calculation. The CRC is the numerical result of this calculation and is held separately from the data. The integrity of the data is checked by calculating a new CRC. If the two CRC's

match, then there is a high degree of confidence that the data has not changed.

Crisis ➤ A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate.

Crisis Management ➤ The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.

Crisis Simulation ➤ The process of testing an organization's ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

Critical Functions ➤ Business activities or information which could not be interrupted without significantly jeopardizing operation of the organization.

Critical Records ➤ Records or documents which, if damaged or destroyed, would cause considerable inconvenience and / or require replacement or recreation at considerable expense.

Cross-Site Scripting ➤ Is a class of attacks made possible by the failure of a web site to validate user input and which results in malicious code being run in a victim's browser. Because of an error in a legitimate site's web code, an attacker is able to get the site to return code from his site to the browser of someone visiting the legitimate site. The victim's browser thinks it's from the legitimate site and executes it.

CSMA/CD (Carrier Sense Multiple Access Collision Detect) ➤ Media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period of time, a device can transmit. If two devices transmit at once, a collision occurs and is detected by all colliding devices. This collision subsequently delays retransmissions from those devices for some random length of time. CSMA/CD access is used by Ethernet and IEEE 802.3.

Daisy Chain ➤ In LocalTalk, a daisy chain is made by linking LocalTalk connectors together with patch cord. In telephony, a daisy chain refers to the method of linking a series of wall outlets together with twisted pair cabling rather than the normal practice of connecting the wall outlets to a central location (home run). In telephony, "daisy chaining" is equivalent to the "backbone" method of LocalTalk construction.

Damage Assessment ➤ The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.

Glossary

DARPA (Defense Advanced Research Projects Agency) ➤ US. government agency that funded research for and experimentation with the Internet. Evolved from ARPA, and then, from 1994, back to ARPA.

Data ➤ In computer terminology facts, information or characters processed, stored or produced by computer.

Data Centre Relocation ➤ The relocation of an organization's entire data processing operation.

Data Dictionary ➤ A tool that stores information about data used in a data base.

Data Link Layer ➤ Layer 2 of the OSI reference model. This layer provides reliable transit of data across a physical link. The data link layer is concerned with physical addressing, network topology, line discipline, error notification, ordered delivery of frames, and flow control. The IEEE has divided this layer into two sublayers: The MAC sublayer and the LLC sublayer. Sometimes simply called Link Layer. See also Application Layer, LLC, MAC, Network Layer, Physical Layer, Presentation Layer, Session Layer, and Transport Layer.

Data Link Protocol ➤ The protocol that controls the network signaling and receiving hardware, performing data integrity checks and formatting information according to the rules of the data link.

Data Oriented Systems Development ➤ This technique of development is useful in ad hoc reporting for users by developing a suitable accessible data storage technique

Data Processing (DP) ➤ The arranging of data into a form suited to producing required results; the handling of data in order to classify, sort, calculate and record; and the production and updating of records and reports.

Data Security ➤ Procedures used to protect computer data

Data Vaulting ➤ Contracting with an online service that automatically and regularly connects to a host or hosts and copies identified data to an online server. Typical arrangements can be made to back up everything, data only, or specific datasets.

Database ➤ A database is defined as a centralised repository of all the inter-related information of an organization, designed to meet the needs of many types of user.

Database Administrator (dba) ➤ An information technology expert who is responsible for all the technical operations on a database in an organisation.

- Database Analysers** ➤ Software used by the auditor to examine the rights associated with terminals and the ability of users to access information on a database
- Database Auditing** ➤ Recording specific actions that are performed on a database server. Auditing can be specified at the level of the database server or on specific database objects.
- Database Permissions** ➤ Permissions placed on objects within a database. Database permissions specify which actions a database user can perform on tables, views, stored procedures, and other objects.
- Database Triggers** ➤ Database objects that can be used to automatically execute operations whenever information stored in tables is accessed or modified.
- Database View** ➤ A logical database object that refers to underlying database tables. Views generally do not contain data, do not require storage space, and can be used to better manage security permissions.
- Datagram** ➤ Logical grouping of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms frame, message, packet, and segment are also used to describe logical information grouping at various layers of the OSI reference model and in various technology circles.
- DBMS (Data Base Management Systems)** ➤ Software that manages a database and provides facilities for database creation, populating data, data storage, data retrieval, data access control.
- DCL (Data Control Language)** ➤ DCL statements control a database, including administering privileges and committing data.
- DDL (Data Definition Language)** ➤ DDL statements are used to define a database, build and modify the structure of tables and other objects in the database.
- De Facto Standard** ➤ Standard that exists by nature of its widespread use. Compare with De Jure Standard. See also Standard.
- De Jure Standard** ➤ Standard that exist because of its approval by an official standards body. Compare with De Facto Standard. See also Standard.
- Deadlock** ➤ 1. Unresolved contention for the use of a resource. 2. In an application, when two elements of a process each wait for action by or a response from the other before they resume the process.
- Debugger** ➤ A systems software utility that helps in identifying problems that occur during execution.

Glossary

- Decryption** ➤ The reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state. See also Encryption.
- Dedicated Line** ➤ A pre-established point to point communication link between computer terminals and a computer processor, or between distributed processors, that does not require dial-up access. See also Leased Line.
- Default Route** ➤ Routing table entry that is used to direct frames for which a next hop is not explicitly listed in the routing table.
- Defense** ➤ Protection of physical or electronic information resources and data.
- Defense In Depth** ➤ Utilizing multiple layers of security controls to present several challenges to attackers that must all be compromised sequentially in order to gain unauthorized access.
- Demodulation** ➤ Process of returning a modulated signal to its original form. Modems perform demodulation by taking an analog signal and returning it to its original (digital) form. See also Modulation.
- Demultiplexing** ➤ The separating of multiple input streams that have been multiplexed into a common physical signal back into multiple output streams. See also Multiplexing.
- Denial Of Service (DoS)** ➤ Causing an information resource to be partially or completely unable to process requests. This is usually accomplished by flooding the resource with more requests than it can handle, thereby rendering it incapable of providing normal levels of service.
- Departmental Recovery Team** ➤ A group of individuals responsible for performing recovery procedures specific to their department.
- Detection** ➤ Protective measures intended to reduce the likelihood of a successful compromise of information resources by recognizing that an attack has occurred or is occurring. An IDS system is a detection measure.
- Deterrence** ➤ The use of negative behavior reinforcement to cause would-be attackers either to avoid attempts to breach security or to go elsewhere with their attacks.
- Device Drivers** ➤ A system software which informs the computer how to use a particular peripheral device.
- Diagnostic** ➤ A test or the data from a test which indicates the condition of the state of a computer or health of the network.

- Dial-up Line** ➤ Communications circuit that is established by a switched-circuit connection using the telephone company network.
- Dictionary Attack** ➤ An attack against encrypted ciphertext in which a dictionary, or word list, is used. Each word in the list is encrypted in the same manner that a user password is, and then they are compared to the stored, encrypted passwords. If a match is found, the password is cracked. See also Brute-Force Attack.
- Digital Signatures** ➤ A means of authentication of electronic record involving transformation of the electronic record in plain text using asymmetric cryptography and a hashing function that generates an encrypted message digest, that is independently verifiable at the receiver's end.
- Disaster** ➤ A sudden, unplanned calamitous event causing great damage or loss. In the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time. Similar Terms: Business Interruption; Outage.
- Disaster Mitigation** ➤ Actions and activities to eliminate or reduce the degree of risk to life and property from hazards.
- Disaster Preparedness** ➤ Activities, programs, and systems developed prior to a disaster that are used to support and enhance mitigation, response, and recovery to disasters.
- Disaster Prevention** ➤ Measures employed to prevent, detect, or contain incidents which, if unchecked, could result in disaster.
- Disaster Prevention Checklist** ➤ A questionnaire used to assess preventive measures in areas of operations such as overall security, software, data files, data entry reports, microcomputers, and personnel.
- Disaster Recovery** ➤ Activities and programs designed to return the entity to an acceptable condition.
- Disaster Recovery Administrator** ➤ The individual responsible for documenting recovery activities and tracking recovery progress.
- Disaster Recovery Coordinator** ➤ The Disaster Recovery Coordinator may be responsible for overall recovery of an organization or unit(s). Similar Terms: Business Recovery Coordinator.
- Disaster Recovery Period** ➤ The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.

Glossary

Disaster Recovery Plan ➤ Approved set of arrangements and procedures that enable an organization to respond to a disaster and resume its critical business functions within a defined time frame.

Disaster Recovery Planning ➤ Process of developing advance arrangements and procedures that enable an organization to respond to a disaster and resume the critical business functions within a predetermined period of time, minimize the amount of loss, and repair or replace the damaged facilities as soon as possible. Similar Terms: Contingency planning; business resumption planning; corporate contingency planning; business interruption planning; disaster preparedness.

Disaster Recovery Software ➤ An application program developed to assist an organization in writing a comprehensive disaster recovery plan.

Disaster Recovery Teams (Business Recovery Teams) ➤ A structured group of teams ready to take control of the recovery operations if a disaster should occur.

Disaster Response ➤ Activities designed to address the immediate and short-term effects of the disaster.

Disk-To-Disk (D2D) Technology ➤ Use of a disk array or appliance disk to store data. A slow tape backup system may be a bottleneck, as servers may be able to provide data faster than the tape system can record it. D2D servers don't wait for a tape drive, and disks can be provided over high-speed dedicated backup networks, so both backups and restores can be faster.

Distributed Processing ➤ Use of computers at various locations, typically interconnected via communication links for the purpose of data access and/or transfer.

DML (Data Manipulation Language) ➤ DML statements are used to maintain and query a database.

Documentation ➤ A description of the function of a program or set of programs or a system. Also refers to the working papers prepared or obtained by the auditor and retained by him in connection with the performance of audit.

Dual Homing ➤ Network topology in which a device is connected to the network by way of two independent access points (points of attachment). One access point is the primary connection, and the other is a standby connection that is activated in the event of a failure of the primary connection.

Dynamic Address Resolution ➤ Use of an address resolution protocol to determine and store address information on demand.

- Dynamic Addressing** ➤ A system of addressing in which the computer selects its own address without the user's intervention.
- Dynamic Routing** ➤ Routing that adjusts automatically to network topology or traffic changes. Also called adaptive routing.
- EAM (Embedded Audit Module)** ➤ Refers to software used by the auditor to examine transactions passing through the an application system. This the auditor does by embedding the code containing the audit procedures in the application software of the auditee.
- EBCDIC (Extended Binary-Coded Decimal Interchange Code)** ➤ EBCDIC is an 8-bit code widely used on IBM mainframes.
- Echo Test** ➤ A diagnostic test in which packets are sent by one node to another node, which immediately returns them to the original node. The data recorded by the echo test includes the success rate of the return as well as the time needed to complete the round trip.
- EDI (Electronic Document (Or Data) Interchange)** ➤ the transfer of data between different companies using networks, such as the Internet, where authentication and security methods guarantee the integrity and origin of the information.
- Editor** ➤ A system software utility that allows the user to create and edit files.
- Electromagnetic Interference (EMI)** ➤ Interference in the integrity of a signal caused by radiation. An example is the radiation from a fluorescent light, which emits abroad spectrum of electromagnetic radiation, including radiation that may be harmful to a signal not protected by either shielding or adequate twisting.
- Electronic Mail** ➤ Widely used network application in which mail messages are transmitted electronically between end users over various types of networks using various network protocols. Often called e-mail.
- Electronic Record** ➤ (as per IT Act, 2000) with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.
- Electronic Vaulting** ➤ Transfer of data to an offsite storage facility via a communication link rather than via portable media.
- Elevation Of Privilege** ➤ An attack that enables the attacker to operate code with more rights than normally allowed. Such attacks are the most prized by attackers.

Glossary

- E-Mail** ➤ Electronic Mail. A network application that can deliver messages from one computer user to another.
- Embedded Operating Sytem** ➤ An operating system that can be deployed on embedded devices, which are stripped-down versions of desktop computers.
- Emulation** ➤ A network activity in which a computer acts as if it is another kind of computer or terminal. An example is when a Macintosh user opens a remote terminal session to a VAX, it may run a program that emulates a DEC VT240 terminal.
- Enabling Technologies** ➤ Technologies that complement business functions in such a way as to make the business more effective and profitable and to increase productivity.
- Encapsulation** ➤ 1. In telecommunications, the process of placing one protocol inside of another. Usually implies that the encapsulated protocol was not originally intended by its designers to be carried by the encapsulating protocol. 2. In Object Oriented systems, encapsulation is the process by which every object conceals the internal data and procedures and provide an interface in such a way that they reveal as little as possible about the inner workings.
- Encryption** ➤ The application of a specific algorithm to data so as to alter the appearance of the data making it incomprehensible to those who are not authorized to see the information. See also Decryption.
- Enterprise Network** ➤ A networking system that allows communication and resource sharing among all of a company's business functions and workers. In some circles, this would even include the company's suppliers and distributors.
- Entity** ➤ A hardware (or firmware) device or software process capable of initiating or responding to communication. Entities typically possess a unique address.
- Entropy** ➤ 1. A measure of the disorder of a system. 2. The thermodynamic tendency of a system to reduce its overall energy state by increasing its disorder. Theoretically, an equilibrium is reached where the energy reduction that can be achieved by a further increase in entropy is offset by the energy necessary to contain that increase.
- Equivalent Security** ➤ Security controls that are implemented at an identical level for all information resources and that complement each other in protecting a particular asset by securing the asset as well as all other resources that have access to that asset with the same strength of security. Also called Transitive Security.

- Error Checking** ➤ In data transmission, an action where the integrity of data is verified.
- Error Control** ➤ Technique for detecting and correcting errors in data transmissions.
- Ethernet** ➤ A specification for a transmission system including Layers 1 and 2 of the OSI 7-layer model using the CSMA/CD access method. In common usage, "Ethernet" refers to both the DIX (DEC - Intel - Xerox) version of this specification or to the IEEE version, more formally known as "802.3". The DIX version is distinguished by the reference "Ethernet V.2".
- Expert Systems** ➤ Software that map the expertise of people, learning from their logic and method of making decisions.
- Exposure** ➤ A condition of an information resource that may allow unauthorized access, denial of service, or other successful attacks.
- Extensible Architecture** ➤ A network security architecture that can be scaled to fit the requirements of the business as the business evolves, as opposed to a static network security design that is not flexible.
- Extra Expense Coverage** ➤ Insurance coverage for disaster related expenses which may be incurred until operations are fully recovered after a disaster.
- Extranet** ➤ A network that is outside the control of the company. Extranets are usually connections to outside companies, service providers, customers, and business partners.
- Facilities** ➤ A location containing the equipment, supplies, voice and data communication lines, to conduct transactions required to conduct business under normal conditions. Similar Terms: Primary Site, Primary Processing Facility, Primary Office Facility.
- False-Negative** ➤ An incorrect result as reported by a detective device, such as a IDS or antiviral program or biometric security device. For example, an antiviral program may not 'catch' a viral infected file, or a fingerprint reader may incorrectly fail the fingerprint of the true user.
- False-Positive** ➤ An incorrect result as reported by a detective device. In this case, a harmless attachment to an e-mail is reported as a virus, or an imposter is given access to an account protected by a fingerprint reader.
- Fault Management** ➤ One of five categories of network management defined by ISO for management of OSI networks. Fault management attempts to ensure that network faults are detected and controlled. See also

Glossary

Accounting Management, Configuration Management, Performance, and Security Management.

FDDI (Fiber Data Distributed Interface) ➤ A specification (ANSI X 3T9.5) for 100 MBits/sec. on dual counter-rotating token passing ring implemented on fiber optic cabling.

Feasibility Study ➤ The first phase of the SDLC project that confirms feasibility and adequacy of resources for the development or acquisition process.

Fiber-Optic Cable ➤ Physical medium capable of conducting modulated light transmission. Fiber-optic cable is not susceptible to electromagnetic interference and is capable of higher data rates. Sometimes called Optical Fiber.

Fifth-Generation Language (5GL) ➤ A high level language that has a natural language interface to it.

File System ➤ Refers to the collection of system software routines that manages and accesses files located on a computer's storage volumes.

File Transfer ➤ Popular network application that allows files to be moved from one network device to another.

Finger ➤ A collection of software routines used by computers running the IP protocol stack, which allows a user to read public information about a user on the same, or a remote machine, often including full name, telephone number and extension, snail-mail address, time and place of last login, whether user has any pending unread mail, and witticisms selected by the user.

Fingerprinting ➤ Using software techniques to discover the identity (version, patch level, or operating system) of remote software or hardware. Fingerprinting is often used by malicious hackers in preparation for an attack.

Firewalls ➤ Software and/or hardware devices that are placed at the network perimeter to protect the internal network resources from unauthorized external traffic from coming into the network.

Firmware ➤ A collection of programmed routines and instructions that is implemented in a computer chip or similar hardware form instead of a software form.

First-Generation Language (1GL) ➤ Also called machine language, in which all instructions are given as strings of 0s and 1s.

Flag ➤ In a packet, a bit (or sometimes a group of bits) that indicates a condition. For example, the ZIP GetNetInfo Reply includes a 1-bitflag

that indicates whether the zone name specified either is or is not a valid home zone name for the node that requested the information.

Flash Memory > Technology developed by Intel and licensed to other semiconductor companies. Flash memory is nonvolatile storage that can be electrically erased and reprogrammed. Allows software images to be stored, booted, and rewritten as necessary.

Flow Control > Technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

FM (Frequency Modulation) > In data transmission, a system of signaling in which the data is encoded by varying the frequency of the signal.

Fourth-Generation Language (4GL) > Also termed as database languages or report generators. These are non-procedural languages with user-friendly syntax.

Fragment > Piece of a larger packet that has been broken down to smaller units.

Fragmentation > Process of breaking a packet into smaller units when transmitting over a network medium that cannot support a packet of the original size. See also Re-assembly.

Frame > In data networks, the information packet and all of the preceding and succeeding signals necessary (flag bytes, preambles, frame checks, abort sequences, etc.) to convey it along the data link.

Frame Relay > Industry-standard, switched data link layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices. Frame relay is more efficient than X.25, the protocol for which it is generally considered a replacement. See also X.25.

Front End > Node or software program that requests services of a back end. See also Back End, Client and Server.

FTP > File Transfer Protocol. Lowest-common-denominator protocol for the point-to-point transfer of text and binary files between IP connected hosts.

Full Mesh > Term describing a network in which devices are organized in a mesh topology, with each network node having either a physical circuit or a virtual circuit connecting it to every other network node. A full mesh provides a great deal of redundancy, but because it can be prohibitively expensive to implement, it is usually reserved for network backbones. See also Mesh and Partial Mesh.

Glossary

- Full-Duplex** ➤ A communication system between two entities in which either entity can transmit simultaneously.
- Function Point Analysis** ➤ Function points are the factors such as inputs, outputs, logical internal sites etc which determine the size of a software and thus the effort of a developmental task.
- Gateway** ➤ 1. A device that performs a protocol translation at the Session Layer or higher. 2. Archaic. A TCP/IP router that routes packets between different network numbers.
- Generalised Audit Software (GAS)** ➤ Refers to standard software, which can directly read and access data from various database platforms, flat file systems and ASCII formats and can achieve mathematical computations, comparing, sorting, sampling, duplicate check, re-computations, etc.
- GUI (Graphical User Interface)** ➤ User environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored. Conventions such as buttons, icons and windows are typical, and many actions are performed using a pointing device (such as a mouse).
- Hacker** ➤ Either a person who explores computers and networks to discover their capabilities, or a malicious intruder who tries to discover information by gaining unauthorized access and who may make changes or commit hostile acts.
- Half-Duplex** ➤ Capability for data transmission in only one direction at a time between a sending station and a receiving station. Compare with Full-Duplex and Simplex.
- Hardware** ➤ Data processing equipment including a computer system - mainframe, mini or micro and peripheral equipment, such as terminals and line printers
- Header** ➤ In a network packet or frame, a section of data that describes the data that immediately follows.
- Hello Packet** ➤ Multicast packet that is used by routers for neighbor discovery and recovery. Hello packets also indicate that a client is still operating and network-ready.
- Hello Protocol** ➤ Protocol used by OSPF systems for establishing and maintaining neighbor relationships.
- Hertz (HZ)** ➤ A unit of measure of the frequency of cyclic wave form, equal to one cycle or period per second.

- Heterogeneous Network** ➤ Network consisting of dissimilar devices that run dissimilar protocols and in many cases support dissimilar functions or applications.
- Heuristic Attack** ➤ An attack, usually against a password, which attempts to apply knowledge of how users commonly create passwords. It exploits the common ways people think. For example, when asked to add numbers to passwords, users commonly add them to the end of the password. The heuristic attack looks for numbers in the last two digits before looking for characters there. Another example is the use of capital letters. User's commonly capitalize the first character. An example of a seemingly complex password which will be cracked fairly quickly by a heuristic attack is Kopper2.
- Honeypot** ➤ A host-based IDS where the entire system is created solely to monitor, detect and capture security threats against it. See also Intrusion Detection System.
- Host** ➤ In terminal emulation, the remote computer that is being controlled by the terminal emulation software.
- Host-Based IDS (HIDS)** ➤ An IDS used to monitor a single host. Usually a HIDS is software that is installed on the host it protects. See also Intrusion Detection System.
- Hot Site** ➤ Alternate facility with equipment and resources to recover the critical business functions affected by a disaster.
- HTML (Hypertext Markup Language)** ➤ Document formatting language that uses tags to indicate how a given part of a document should be interpreted by a viewing application, such as a WWW browser. See also Hypertext and WWW browser.
- Hub** ➤ 1. Generally, a term used to describe a device that serves as the center of a star-topology network. 2. Hardware devices that contain multiple independent but connected modules of network and internetwork equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat, but merely split, signals sent through them). 3. In Ethernet and IEEE 802.3, an Ethernet multiport repeater, sometimes referred to as a concentrator.
- Human Threats** ➤ Possible disruptions in operations resulting from human actions (disgruntled employee, terrorism, etc.).
- Hybrid Network** ➤ Internetwork made up of more than one type of network technology, including LANs and WANs or network, which is based on multiple topologies.

Glossary

- Hypertext** ➤ Electronically-stored text that allows direct access to other texts by way of encoded links. Hypertext documents can be created using HTML, and often integrate images, sound, and other media that are commonly viewed using a WWW browser. See also HTML and WWW browser.
- IEEE (Institute Of Electrical And Electronic Engineers)** ➤ A non-profit organization that, among many other activities, endeavors to coordinate, synthesize and promote data networking standards.
- IEEE 802.1** ➤ IEEE specification that describes an algorithm that prevents bridging loops by creating a spanning tree. The algorithm was invented by Digital Equipment Corporation. The Digital algorithm and the IEEE 802.1 algorithm are not exactly the same, nor are they compatible. See also Spanning Tree, Spanning-Tree Algorithm, and Spanning-Tree Protocol.
- IEEE 802.12** ➤ IEEE LAN standard that specifies the physical layer and the MAC sublayer of the data link layer. IEEE 802.12 uses the demand priority media-access scheme at 100 Mbps over a variety of physical media. See also 100VG-AnyLAN.
- IEEE 802.2** ➤ The committee of the IEEE charged with the responsibility of coordinating standards at the Data Link Layer. The committee also oversees the work of many sub-committees that govern individual Data Link standards such as the 802.3 standard.
- IEEE 802.3** ➤ IEEE LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet. Physical variations of the original IEEE 802.3 specifications include 10Base2, 10Base5, 10BaseF, 10BaseT, and 10Broad36. Physical variations for Fast Ethernet include 100BaseT, 100BaseT4, and 100BaseX.
- IEEE 802.4** ➤ IEEE LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data link layer. IEEE 802.4 uses token-passing access over a bus topology and is based on the token bus LAN architecture. See also Token Bus.
- IEEE 802.5** ➤ IEEE LAN protocol that specifies an implementation of the physical layer and MAC sublayer of the data link layer. IEEE 802.5 uses token passing access at 4 or 16 Mbps over STP cabling and is similar to IBM Token Ring. See also Token Ring.
- Impedance** ➤ A measure of the opposition to the flow of an alternating signal by its media.

- Incident Management** ➤ Process of instituting and managing systems and procedures to identify security breaches for appropriate response to prevent or detect and correct risks arising therefrom
- Incremental Testing** ➤ Involves testing only value added functionality of the software components.
- Information** ➤ The meaning assigned to data by means of conversions applied to that data.
- Information Resources** ➤ Software, web browsers, e-mail, computer systems, workstations, PCs, servers, entities connected on the network, data, telephones, voice mail, fax machines, and any information that could be considered valuable to the business.
- Information Security** ➤ The practice of protecting information in all its forms, whether written, spoken, electronic, graphical, or using other methods of communication.
- Information Systems** ➤ Denotes the computers, communications facilities and data and information that may be recorded, processed, stored, shared, transmitted, or retrieved by them, including programs, specifications, and procedures for their operation, use, and maintenance.
- Information Systems Auditor** ➤ Is a person with knowledge of audit procedures and information systems, who ensures that the information system is adequate in terms of confidentiality, integrity and availability for the specified business purpose
- Information Technology (IT)** ➤ Encompasses hardware and software products, information system operations and management processes, and the human resources and skills required to apply those products and processes to the task of information production and information system development, management and control.
- Infrared** ➤ 1. A portion of electromagnetic spectrum situated between visible light and microwaves. 2. A means of short distance wireless networking that depends on an unobstructed line of sight path.
- Inherent Risk** ➤ Risks inherent in the very nature of the system or operation of the system, which individually by themselves may appear to be harmless but if combined with other similar risks or lack of controls may cause material impact.
- Integrity** ➤ The characteristic of data and information being accurate and complete and the preservation of accuracy and completeness by protecting the data and information from unauthorized, unanticipated, or unintentional modification.

Glossary

- Interface Testing** ➤ Involves the testing of the interfaces between two modules of a software.
- Internal Control** ➤ Any policy, procedure or activity which promotes the protection of assets, accuracy of financial data, operational efficiency, and enforces compliances with company policies and procedures
- Internal Hot-Sites** ➤ A fully equipped alternate processing site owned and operated by the organization.
- Internet** ➤ The worldwide system of linked networks that is capable of exchanging mail and data through a common addressing and naming system based on TCP/IP protocols.
- Internet Address** ➤ An address that identifies a communication entity on an internet.
- Interpreter** ➤ A translator that takes a 3GL code as an input and produces corresponding machine code as output. Unlike a compiler, an interpreter translates each program statement into machine code just before the program statement is executed.
- Intrusion Detection System (IDS)** ➤ A hardware appliance or software designed to detect, alert on, and report malicious attacks and unauthorized misuse on a network or host. An IDS does not do anything about the attack, it simply raises an alert.
- Intrusion Prevention System (IPS)** ➤ Either an in-line device that examines network activity passing through it, dropping any communications that are identified as malicious, or software that resides on a computer system that blocks activity identified as inappropriate (such as buffer overflows, memory allocation violations, and so on). Unlike an IDS, the IPS responds to an attack with some action. The IDS simply reports it.
- ISDN (Integrated Services Digital Network)** ➤ Communication protocol, offered by telephone companies, that permits telephone networks to carry data, voice, and other source traffic.
- IT Governance** ➤ As per the Information Technology Governance Institute, refers to a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk over IT and its processes.
- Kernel** ➤ Core part of an operating system which deals with the basic system resources. The kernel drives physical devices and handles I/O, memory management and process scheduling.
- LAN** ➤ A communication infrastructure that supports data and resource sharing within a small area that is completely contained on the premises of a single owner.

- LAN Recovery** ➤ The component of Disaster Recovery which deals specifically with the replacement of LAN equipment in the event of a disaster, and the restoration of essential data and software. Similar Terms: Client / Server Recovery
- LAN Server** ➤ A general term used to describe a device that manages and allows the use of more than one kind of resource such as storage or file services, print services, communication services, data base services, etc.
- LAN Switch** ➤ High-speed switch that forwards packets between data-link segments. Most LAN switches forward traffic based on MAC addresses. This variety of LAN switch is sometimes called a frame switch. LAN switches are often categorized according to the method they use to forward traffic: cut-through packet switching or store-and-forward packet switching. Multilayer switches are an intelligent subset of LAN switches. Compare with Multilayer Switch. See also Cut-through Packet Switching and Store and Forward Packet Switching.
- Laser (Light Amplification By Simulated Emission Of Radiation)** ➤ Analog transmission device in which a suitable active material is excited by an external stimulus to produce a narrow beam of coherent light that can be modulated into pulses to carry data.
- Leased Line** ➤ Usually synonymous with dedicated line. See Dedicated Line
- Line Rerouting** ➤ A service offered by many regional telephone companies allowing the computer centre to quickly reroute the network of dedicated lines to a backup site.
- Linker** ➤ A systems software that does the process of combining various pieces of code and data together to form a single executable unit that can be loaded in memory.
- Load Balancing** ➤ In routing, the ability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the utilization of network segments, thus increasing effective network bandwidth.
- Loader** ➤ A systems software that loads the code and data of the executable object file into the main memory, goes to the very first instruction and then executes the program.
- Log Analyzers** ➤ Software used by the auditor to read and analyse records of machine activity

Glossary

- Login** ➤ A formal procedure where a computing device initiates a sustained connection to another computing device for the purpose of using a resource managed by the computer.
- Logout** ➤ A Formal procedure where a computing device severs its connection to another computing device.
- Loop Route** ➤ In a loop route, packets never reach their destination, but simply cycle repeatedly through a constant series of network nodes.
- Loss** ➤ Unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may include loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.
- Loss Reduction** ➤ The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction is intended to react to an event and limit its effect. Examples of Loss Reduction include sprinkler systems, insurance policies and evacuation procedures.
- MAC Address** ➤ Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, a MAC-layer address, or a physical address.
- Macro Virus** ➤ A computer virus written using an application's macro language. See also Appending Virus, Boot Virus, Memory-Resident Virus, Multipartite Virus, Nonresident Virus, Overwriting Virus, Parasitic Virus, Prepending Virus, Stealth Virus, and Virus.
- Mainframe Computer** ➤ A mainframe computer is a large and fast computer with powerful data processing capabilities.
- Malware** ➤ Malicious software.
- Management Console** ➤ A central computer or device used to collect or report on data from one or more distributed devices.
- Mappers** ➤ Software used by the auditor to list unused program instructions
- Master Data** ➤ Information which does not undergo change for a fairly long period.
- MBone** ➤ Multicast backbone. The multicast backbone of the Internet. MBone is a virtual multicast network composed of multicast LANs and the point-to-point tunnels that interconnect them.

- Media Transportation Coverage** ➤ An insurance policy designed to cover transportation of items to and from an EDP centre, the cost of reconstruction and the tracing of lost items.
- Memory Dump** ➤ involves copying raw data from one place to another with little or no formatting for readability.
- Memory-Resident Virus** ➤ A computer virus that remains in active memory after the host program is finished executing.
- Mesh Network** ➤ Topology in which devices are organized in a manageable, segmented manner with many, often redundant, interconnections strategically placed between network nodes.
- Message** ➤ Application layer (Layer 7) logical grouping of information, often composed of a number of lower-layer logical groupings such as packets. The terms datagram, frame, packet, and segment are also used to describe logical information groupings at various layers of the OSI reference model.
- Message Switching** ➤ Switching technique involving transmission of messages from node to node through a network. The message is stored at each node until such time as a forwarding path is available.
- Metadata** ➤ Information stored within an assembly concerning the classes defined in that assembly (such as names and types of fields, method signatures, dependence on other classes, and so on).
- Micro-Computers** ➤ Also known as Personal Computers, popularly called as a PC, or Desktop machines. Stand-alone machines based on a single microprocessor chip and are single user systems.
- Microwave** ➤ 1. Any electromagnetic radiation with a wavelength between 1 millimeter and 1 meter. 2. A point-to-point data transmission system employing electromagnetic radiation using a carrier frequency in the microwave region.
- Mini Computer** ➤ A Mini Computer is a scaled down version of a mainframe machine, designed to meet the computing needs of a small and medium enterprises (SME).
- MIPS (Millions Of Instructions Per Second)** ➤ Unit for number of instructions executed by a processor per second.
- Misuse** ➤ Any activity that is unauthorized , and which may or may not include specially crafted code or techniques.
- Mitigate** ➤ To make milder, less severe, or less painful.

Glossary

- Mobile Hot Site** ➤ A large trailer containing backup equipment and peripheral devices delivered to the scene of the disaster. It is then hooked up to existing communication lines.
- Modulation** ➤ Process by which the characteristics of electrical signals are transformed to represent information. Types of modulation include AM, FM, and PAM.
- Mosaic** ➤ Public-domain WWW browser, developed at the National Center for Supercomputing Applications (NCSA).
- Motherboard** ➤ The main circuit board of a microcomputer that contains the CPU, BIOS, memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers required to control standard peripheral devices, such as the display screen, keyboard, and disk drive.
- MSAU** ➤ Multistation access unit. Wiring concentrator to which all end stations in a Token Ring network connect. The MSAU provides an interface between these devices and the Token Ring interface.
- Multicast** ➤ Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the destination address field.
- Multidrop (Line)** ➤ Communications line having multiple cable access points. Sometimes called a Multipoint Line.
- Multihomed (Host)** ➤ Host attached to multiple physical network segments in an OSI CLNS network.
- Multihoming** ➤ Addressing scheme in IS-IS routing that supports assignment of multiple area addresses.
- Multipartite Virus** ➤ A computer virus with more than one vector of attack; for example, a virus that infects boot sectors and file executables. See also Appending Virus, Boot Virus, Macro Virus, Memory-Resident Virus, Nonresident Virus, Overwriting Virus, Parasitic Virus, Prepending Virus, Stealth Virus, and Virus.
- Mutual Authentication** ➤ In this process, not only does the client authenticate to the server, but the server also proves its identity to the client.
- Name Caching** ➤ Method by which remotely discovered host names are stored by a router for use in future packet-forwarding decisions to allow quick access.
- Name Server** ➤ Server connected to a network that resolves network names into network addresses.

- Natural Threats** ➤ Events, caused by nature, causing disruptions to an organization.
- NetBIOS** ➤ Network Basic Input / Output System. API used by applications on an IBM LAN to request services from lower-level network processes. These services might include session establishment and termination, and information transfer.
- Netware** ➤ A trademark of Novell that includes network operating systems and LAN server processes that run on and/or serve many computing platforms, operating systems and protocols.
- Network Adapter** ➤ A hardware device that translates electronic signals between a computing device's native network hardware and the transmission media. A network adapter may also include memory or additional hardware or firmware to aid or perform the computing device's network operations.
- Network Address** ➤ Network layer address referring to a logical, rather than a physical, network device. Also called a Protocol Address.
- Network Administrator** ➤ A person who is charged with the responsibility of caring for a network and the communication abilities of its users.
- Network Analyzer** ➤ Hardware or software device offering various network troubleshooting features, including protocol-specific packet decodes, specific pre-programmed troubleshooting tests, packet filtering, and packet transmission.
- Network Architecture** ➤ A set of specifications that defines every aspect of a data network's communication system, including but not limited to the types of user interfaces employed, the networking protocols used and the structure and types of network cabling that may be used.
- Network Interface Boundary** ➤ Between a carrier network and a privately-owned installation
- Network Layer** ➤ Layer 3 of the OSI reference model. This layer provides connectivity and path selection between two end systems. The network layer is the layer at which routing occurs.
- Network Management** ➤ A set of activities and duties whose goal is to provide high-quality, reliable communication among a group of networked computer users. Typical activities may include resource planning, network design, providing user assistance and training, reconfiguration of the network due to a change in user requirements, assessing user needs and designing appropriate solutions and troubleshooting and remedying network problems as they arise.

Glossary

- Network Outage** ➤ An interruption in system availability as a result of a communication failure affecting a network of computer terminals, processors, or workstations.
- Network-Based IDS (NIDS)** ➤ A hardware or software system designed to detect malicious threats by capturing and analyzing network packets.
- NFS** ➤ Network File System. A file meta-language and set of procedure calls to access and manage files that is standard on nearly every computer that uses TCP/IP protocols as its standard network protocols. Designed by Sun Microsystems, NFS is now a standard feature of nearly all Unix systems.
- NIST** ➤ National Institute of Standards and Technology. Formerly the NBS, this U.S. government organization supports and catalogs a variety of standards.
- Non-Repudiation** ➤ A characteristic of a message or a system that prevents the sender from being able to deny sending the message
- Nonresident Virus** ➤ A computer virus that does not stay in memory after its execution. It runs and then deactivates until the next time the host executable is run. See also Appending Virus, Boot Virus, Macro Virus, Memory-Resident Virus, Multipartite Virus, Overwriting Virus, Parasitic Virus, Prepending Virus, Stealth Virus, and Virus.
- Notebook Computers** ➤ Notebook Computers are lightweight machines which are more preferred by mobile users which combine the power of a PC with mobility.
- Object-Level Security** ➤ Security permissions that are applied to specific database objects. For example, a database administrator might allow certain users to update name and address information within the “Employee” database table.
- Off-Site Storage Facility** ➤ A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored for use during disaster recovery.
- One-Time Password System** ➤ A system in which passwords are used once only, each time the user authenticates.
- Onion Model** ➤ A layered security strategy, sometimes referred to as defense in depth, that includes the “strong wall” principle of the lollipop model, but goes beyond the idea of a simple barrier by providing multiple layers of security that must be passed. See also Defense in Depth
- On-Line Systems** ➤ An interactive computer system supporting users over a network of computer terminals.

- Operating Systems (OS)** ➤ A systems software that manages various resources of the machine.
- OSI 7-Layer Model** ➤ A method of describing the relationships between network protocols by grouping them according to the communication functions the protocols provide. The OSI model defines 7 distinct categories (layers) that act successively on data as it makes its way between the user and the transmission media.
- Output Analyzer** ➤ Checks the accuracy of the results of the test run by comparing the actual output of the test data input with the expected output.
- Overwriting Virus** ➤ A computer virus that permanently writes itself over the host file or a portion of the host file during infection. Damage is not easily repairable. See also Appending Virus, Boot Virus, Macro Virus, Memory-Resident Virus, Multipartite Virus, Nonresident Virus, Parasitic Virus, Prepending Virus, Stealth Virus, and Virus.
- Packet** ➤ A discrete chunk of communication in a pre-defined format.
- Palmtops** ➤ A machine that is extremely convenient to carry and offer features such as PIM (Personal Information Manager) that are needed the most by mobile users.
- Parallel Simulation** ➤ Technique used to ensure that the application program used for the live processing is the same as the program authorized. The same input is run through the two copies of the program, one which is being used in the live environment and the other which is available in the library, and the output of both the parallel runs is compared.
- Parallel Test(-ing)** ➤ Testing of the new system vis a vis the existing system with the same data.
- Parasitic Virus** ➤ A computer virus that inserts itself into a host file without overwriting the host file's original contents. See also Appending Virus, Boot Virus, Macro Virus, Memory-Resident Virus, Multipartite Virus, Nonresident Virus, Overwriting Virus, Prepending Virus, Stealth Virus, and Virus.
- Parity Checking** ➤ A method of error checking where an extra bit is used to signify the condition of a small group of data bits.
- Password History** ➤ The remembering of previous passwords by the system, forcing the user to create new passwords.
- Payload** ➤ The damage routine in malware. See also Malware.

Glossary

- Peer** ➤ In networking, a device to which a computer has a network connection that is relatively symmetrical, i.e. where both devices can initiate or respond to a similar set of requests.
- Perimeter Security** ➤ The technologies, hardware and software, operations, staff, and services that address perimeter defenses to prevent unauthorized connections from outside the perimeter (as opposed to controlling access inside) by controlling network access (using firewalls, vulnerability scanners, and virus detectors), by controlling remote access for traveling computers, and by controlling internal and external network connections with different levels of trust.
- Peripheral** ➤ Any hardware resource used by a computer that is external to a computer's enclosure case that is accessed by serial or parallel connections or bus architectures
- Permissions** ➤ Operations that can be applied to or done with an object. Examples of file permissions are read, write, delete.
- Physical Address** ➤ A synonym for Hardware Address or MAC - layer address.
- Physical Layer** ➤ The physical layer is the bottom layer of the seven-layer OSI networking architecture model. It establishes the physical interface and mechanisms for placing a raw stream of bits onto the wire. It defines the voltage, current, modulation, bit synchronization, connection activation and deactivation, and various electrical characteristics for the transmission media (such as unshielded or shielded twisted-pair cabling, coaxial cabling, and fiber-optic cabling).
- Physical Safeguards** ➤ Physical measures taken to prevent a disaster, such as fire suppression systems, alarm systems, power backup and conditioning systems, access control systems, etc.
- Plaintext** ➤ Text that has not been encrypted.
- Polling** ➤ A means of Media Access Control where a device may only transmit information when it is given permission to transmit by a controller device.
- Polymorphism** ➤ In Object Oriented technology, this is a property by which objects can take on or assume many different forms.
- PPP (Point-To-Point Protocol)** ➤ A specification for synchronous or asynchronous data communication between two routers or between a computer system and a network.
- Prepending Virus** ➤ A computer virus that places itself at the beginning of a host file. See also Appending Virus, Boot Virus, Macro Virus, Memory-Resident Virus, Multipartite Virus, Nonresident virus, Overwriting Virus, Parasitic Virus, Stealth Virus, and Virus.

- Presentation Layer** ➤ The presentation layer structures data that is passed down from the application layer into a format suitable for network transmission. This layer is responsible for data encryption, data compression, character set conversion, interpretation of graphics commands, and so on. The network redirector also functions at this layer.
- Print Spooler** ➤ A Software process that accepts a print job from a workstation as if it were a printer and then sends the print job to an actual printer at a later time. There are two styles, a background spooler, where the print spooling process is resident in the same node as the process seeking the print service, and a hardware spooler, where the print spooling process is in a separate node.
- Privacy** ➤ Keeping information as a secret, known only to the originators of that information. This contrasts with confidentiality, in which information is shared among a select group of recipients. See also Confidentiality.
- Privileges** ➤ A process that can be performed on a system, such as shut it down, or log on to it remotely.
- Procedural Safeguards** ➤ Procedural measures taken to prevent a disaster, such as safety inspections, fire drills, security awareness programs, records retention programs, etc.
- Production Programs** ➤ Programs used to process the live data.
- Program Evaluation And Review Technique (PERT)** ➤ Network diagramming technique for monitoring of projects.
- Program Flowcharts** ➤ Diagrammatic representation of program logic
- Programmer** ➤ A person who develops or codes computer programs using a programming language.
- Proprietary** ➤ Meaning that information concerning the methods or implementation of a technology are owned by an individual or a company. "Proprietary" may mean that the information is secret or that the information must be licensed from the owner before it can be used.
- Protocol** ➤ A set of guidelines defining network traffic formats for the easy communication of data between two hosts.
- Protocol Stack** ➤ A group of protocols, usually specified by a single vendor or organization, that are implemented at more than one Layer of the OSI 7-Layer model that also have Service Access Points defined.

Glossary

- Prototyping** ➤ Technique that enables the programmers to show the feel of the application program to the user by developing the screens or reports without actually fully developing the program.
- Radio Frequency (RF)** ➤ 1. Electromagnetic radiation with a frequency in the range of 10 KHz to 300 GHz. 2. Wireless data communication using such radiation.
- Real-Time System** ➤ A system where, when transactions arrive, they are processed immediately, output is shown to the user and the system takes corrective steps, if needed.
- Recovery Action Plan** ➤ The comprehensive set of documented tasks to be carried out during recovery operations.
- Recovery Alternative** ➤ The method selected to recover the critical business functions following a disaster. In data processing, some possible alternatives would be manual processing, use of service bureaus, or a backup site (hot or cold-site).
- Recovery Capability** ➤ This defines all of the components necessary to perform recovery. These components can include a plan, an alternate site, change control process, network rerouting and others.
- Recovery Management Team** ➤ A group of individuals responsible for directing the development and on-going maintenance of a disaster recovery plan. Also responsible for declaring a disaster and providing direction during the recovery process.
- Recovery Planning Team** ➤ A group of individuals appointed to oversee the development and implementation of a disaster recovery plan.
- Recovery Time** ➤ The period from the disaster declaration to the recovery of the critical functions.
- Recovery Time Objective (RTO)** ➤ The maximum acceptable length of time that can elapse before the lack of a business function severely impacts the business entity. The RTO is comprised of two components: the time before a disaster is declared, and the time to perform tasks (documented in the disaster recovery plan) to the point of business resumption.
- Redundancy** ➤ The assurance of availability by providing duplicate systems or alternative processes. See also Availability.
- Regression Testing** ➤ Technique used to retest logical errors or program abends during the initial testing phase.
- Repeater** ➤ A Physical Layer device which restores, amplifies, re-clocks or otherwise improves a network signal that it receives on one of its ports and transmits the improved signal without buffering or interpreting it.

- Requirement Definition** ➤ This is a phase in SDLC where the users define their requirements of the computer system.
- Residual Risk** ➤ The risk that is left after risks which need to be controlled have been identified and appropriate mitigation measures put in place. The management may choose not to implement controls for such risks depending on the risk appetite of the management, cost of controls or the inherent nature of the risks.
- Ring** ➤ A type of network topology where the devices are connected to a continuous conductor.
- Risk** ➤ The potential that a given threat will exploit vulnerabilities of an asset or a group of assets to cause loss or damage to the assets,
- Risk Assessment / Analysis** ➤ Process of identifying the assets, threats affecting the assets, vulnerabilities and the resulting potential impact and its objective assessment.
- Risk Assessment/Analysis** ➤ The process of identifying and minimizing the exposures to certain threats which an organization may experience. Similar Terms: Risk assessment, impact assessment, corporate loss analysis, risk identification, exposure analysis, exposure assessment. Similar Terms: Risk Assessment, Impact Assessment, Corporate Loss Analysis, Risk Identification, Exposure Analysis, Exposure Assessment.
- Risk Elimination** ➤ Processing a risk by preventing the risk from occurring by eliminating a vulnerability, eliminating all threats, reducing the cost of a realized threat to zero, or increasing the effectiveness of security measures to 100 percent.
- Risk Management** ➤ the dynamic process of assessing risks and their classification into acceptable and residual risks and taking appropriate actions to implement and fine tune controls. See also Risk, Threat, and Vulnerability.
- Risk Mitigation** ➤ Processing a risk by controlling its likelihood, its cost, or its threats, through the use of security measures designed to provide these controls. See also Risk and Threat.
- Risk Transference** ➤ Processing a risk by transferring all or part of the cost of the risk to a third party (most commonly an insurance provider). See also Risk.
- Role-Based Security** ➤ The practice of authorising access to a resource on the basis of the user's identity.

Glossary

- Router** ➤ A device that forwards packets between networks according to the rules of a network layer protocol such as DDP and information it has gathered during its service concerning the structure of the internet.
- Rule Set** ➤ Groups of related rules.
- Rule-Based Authorization** ➤ Uses rules that stipulate what a specific user can do on a system.
- Salvage & Restoration** ➤ The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc. following a disaster.
- Salvage Procedures** ➤ Specified procedures to be activated if an equipment or a facility should suffer any destruction.
- Sample Plan** ➤ A generic disaster recovery plan that can be tailored to fit a particular organization.
- Scalability** ➤ The suitability of a system to operate properly and efficiently when configured on a large scale.
- Scope** ➤ Predefined areas of operation for which a plan is developed.
- Script** ➤ A set of instructions that a computer can operate. Unlike a program, script instructions are not compiled into machine language but are interpreted by the system at the time of execution.
- SCSI (Small Computer Systems Interface)** ➤ A specification (ANSI X3T9.2) for a short distance (6 meters max.) Local Area Network using bus topology for up to eight devices.
- Second-Generation Language (2GL)** ➤ Also called Assembly Level language, in which instead of 0s and 1s, mnemonics and operation codes (op-codes) are used as instruction inputs.
- Security** ➤ The practice of protecting assets. This is the fundamental level of the security hierarchy, of which information security, data security, and network security are branches.
- Security Control** ➤ Any technique, technology, activity, or practice that is intended to protect assets.
- Security Policy** ➤ The set of decisions that govern security controls.
- Security Strategy** ➤ The proactive plan of action governing the implementation of a security infrastructure.
- Segmentation** ➤ Splitting a network into different areas using routers and switches, also often accomplished using virtual LAN (VLAN) technology along with access control lists (ACLs). See also Access Control List and VLAN.

- Segregation Of Duties** ➤ Assigning incompatible duties or functions to separate people to provide reasonable assurance against fraud and provide an accuracy check of the other person's work
- Server** ➤ A device that is shared by several users of a network.
- Service Bureau (Center)** ➤ A data processing utility that provides processing capability, normally for specialized processing, such as payroll.
- Session** ➤ An on-going relationship between two computing devices involving the allocation of resources and sustained data flow.
- Session Layer** ➤ The layer in the OSI 7-Layer Model that is concerned with managing the resources required for the session between two computers.
- Shoulder-Surfing** ➤ Using direct observation techniques, such as looking over someone's shoulder, to obtain information. This is normally done casually to avoid being noticed.
- Signature** ➤ Predefined patterns of bytes identifying particular threats.
- Signature-Detection IDS** ➤ An IDS system that works by comparing captured traffic against databases of known bad patterns. Also known as misuse detection. See also Intrusion Detection System and Host-based IDS.
- Simputer** ➤ The Simputer is a low cost portable alternative to PCs, designed by the scientists of Indian Institute of Science, Bangalore with private sector participation.
- Simulation Test** ➤ A test of recovery procedures under conditions approximating a specific disaster scenario. This may involve designated units of the organization actually ceasing normal operations while exercising their procedures.
- Single Sign-On** ➤ A process that can allow the user to only have one logon account and password in order to access all systems on their network.
- Skills Inventory** ➤ A listing of employees which lists their skills that apply to recovery.
- SLIP (Serial Line Internet Protocol)** ➤ A protocol for carrying IP information over serial links.
- SMTP (Simple Mail Transfer Protocol)** ➤ The standard protocol for exchanging mail over TCP/IP networks.
- Snapshots** ➤ Software used by the auditor to take a "picture" of a file of data or a transaction passing through the system at a particular point in time

Glossary

- Sniffing** ➤ The capturing of network packets not intended for the host doing the capturing. This can be used maliciously to discover unauthorized information. Also known as packet capturing or protocol analyzing.
- SNMP (Simple Network Management Protocol)** ➤ A de facto standard for management of networked devices using a simple request-response data retrieval mechanism.
- Software** ➤ A generic term for programs, including both applications programs (for example, payroll, debtors) and systems programs (for example, operating systems and compilers)
- SONET (Synchronous Optical Network)** ➤ A standard for a worldwide digital network using a common transport. SONET can run over copper or fiber.
- Source Code** ➤ Program written using a programming language.
- SQL (Structured Query Language)** ➤ A fourth general language that is very user friendly and used for defining and manipulating databases.
- SQL Engine** ➤ A translator that takes a SQL statement as the input and produces corresponding machine code.
- StarTopology** ➤ LAN topology in which end points on a network are connected to a common central switch by point-to-point links. Compare with Bus Topology, Ring Topology, and Tree Topology.
- Stateful** ➤ Describes a network protocol that uses flags to communicate various session conditions (such as when establishing a session, acknowledging, closing, and so on).
- Stateless** ➤ Describes a network protocol that does not communicate session states during communications (such as UDP).
- StaticRoute** ➤ Route that is explicitly configured and entered into the routing table. Static Routes take precedence over routes chosen by dynamic routing protocols.
- Statistical Multiplexing** ➤ Technique in which information from multiple logical channels can be transmitted across a single physical channel. Statistical multiplexing dynamically allocates bandwidth only to active input channels, making better use of available bandwidth and allowing more devices to be connected than with other multiplexing techniques. Also referred to as Statistical Time-Division Multiplexing or Statmux.
- Stealth Virus** ➤ A computer virus coded to avoid inspection. See also Appending Virus, Boot Virus, Macro virus, Memory-Resident Virus, Multipartite Virus, Nonresident Virus, Overwriting Virus, Parasitic Virus, Prepending Virus, and Virus.

- Steering Committee** ➤ Group of senior managers appointed by the top management to facilitate, monitor and oversee information systems deployment in the enterprise
- Sticky Honeypot** ➤ A honeypot built to attract malicious threats, and to keep them and slow them down from attacking other legitimate hosts. See also Honeypot.
- Stored Procedure** ➤ A database object that can contain executable database server logic. Permissions can be assigned to stored procedures in order to prevent unwanted data modifications and to provide more granular control of security.
- Stream Cipher** ➤ A cryptographic algorithm that operates on a stream of characters.
- Strong Security** ➤ Security controls that approach being completely effective. See also Weak Security.
- Structured Walk-Through Exercise / Test** ➤ Simulated method used to exercise or test a completed disaster recovery plan. Team members meet to walk through each step of the plan verbally to confirm the plan effectiveness and identify gaps, bottlenecks or any other plan weaknesses.
- Subnet Address** ➤ Portion of an IP address that is specified as the subnetwork by the subnet mask. See also Subnet Mask, and Subnetwork.
- Subnet Mask** ➤ A representation of a user's Internet address where all of the bit positions corresponding to the user's network and subnetwork id are 1's and the bit corresponding to the user's host id are 0's.
- Subnetwork** ➤ 1. In IP networks, a network sharing a particular subnet address. Subnetworks are networks arbitrarily segmented by a network administrator in order to provide a multilevel, hierarchical routing structure while shielding the subnetwork from the addressing complexity of attached networks. Sometimes called a subnet. 2. In OSI networks, a collection of ESs and ISs under the control of a single administrative domain and using a single network access protocol.
- Supercomputers** ➤ Very large computers with high processing speed. Designed for specialized applications requiring extensive processing power (such as complex mathematical calculations).
- Switch** ➤ A device that forwards packets between nodes based on the destination node address (either hardware or protocol) of the packet, typically with a buffer time longer than a repeater but shorter than the transmission time of the packet.
- Switched LAN** ➤ LAN implemented with LAN switches.

Glossary

- Synchronous Transmission** ➤ Term describing digital signals that are transmitted with precise clocking. Such signals have the same frequency, with individual characters encapsulated in control bits (called start bits and stop bits) that designate the beginning and end of each character. Compare with Asynchronous Transmission.
- System Flowcharts** ➤ Graphical representation of the sequence of steps in a computer program. These show as to how the data from the source documents shall flow through the computer system to produce output for the distribution to the users.
- System Outage** ➤ An unplanned interruption in system availability as a result of computer hardware or software problems, or operational problems.
- Systems Software** ➤ These refer to the set of programs that enable the system to work, control its working, provide facilities to the programmer to develop application programs, enable various I/O devices to be connected and help in efficient use of the computer resources. Examples are Operating Systems, Programming languages, Device drivers, and Utilities.
- Systems Analyst** ➤ A person skilled in problem definition and analysis who examines a business or industrial situation and designs a computer system to meet the information and operations needs of the business situation
- Systems Development Process** ➤ An approach used to plan, design, develop, test and implement an application system.
- Systems Software** ➤ software used in developing and operating the IT technical components. e.g. operating systems, database management systems, drivers, systems utilities etc.
- T-1** ➤ A Telecommunications technology for wide area networks (WAN) with a transmission speed of 1.554 MBPS over 24 multiplexed 56 Kbps channels.
- T-2** ➤ Four multiplexed T-1 lines offering a communication channel at 6.3 Mbps Available
- T-3** ➤ Twenty-eight multiplexed T-1 circuits with a bandwidth of 44.736 Mbps
- TCP** ➤ Transmission Control Protocol. A reliable Transport Layer Protocol for managing IP that supports re-transmission, sequencing and fragmentation.
- TCP/IP** ➤ Transmission Control Protocol/Internet Protocol. A Transport and Network Layer Protocol respectively, used by a large number of computers.

- TDM** ➤ Time-Division Multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single wire based on pre-assigned time slots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.
- Telex** ➤ Teletypewriter service allowing subscribers to send messages over the PSTN.
- Telnet** ➤ A process to access a remote computer system, often a Unix system, over the network.
- Temporary Operating Procedures** ➤ Predetermined procedures which streamline operations while maintaining an acceptable level of control and auditability during a disaster situation.
- Terminal** ➤ Simple device at which data can be entered or retrieved from a network. Generally, terminals have a monitor and a keyboard, but no processor or local disk drive.
- Terminal Access Controller Access Control System** ➤ Authentication protocol, developed by the DDN community, that provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.
- Terminal Adapter** ➤ Device used to connect ISDN BRI connections to existing interfaces such as EIA/TIA-232. Essentially, an ISDN modem.
- Terminal Emulation** ➤ A computing activity in which a computer runs an application and communicates with a host as if it were a terminal such as a DEC VT220.
- Terminator** ➤ Typically, a resistor placed at the end of a bus to prevent the reflection of signals.
- Test Data** ➤ Data used for testing application software to ensure that the application would not result in erroneous processing and would function as intended by the user..
- Test Plan** ➤ The recovery plans and procedures that are used in a systems test to ensure viability. A test plan is designed to exercise specific action tasks and procedures that would be encountered in a real disaster.
- Thick Ethernet** ➤ Also known as 10Base5.
- Thinnet** ➤ Term used to define a thinner, less expensive version of the cable specified in the IEEE 802.3 10Base2 standard.

Glossary

- Third-Generation Language(3GL)** ➤ Also termed as procedure-oriented language, in which instructions are given in a structured way that resembles English language.
- Threat** ➤ Event that causes a risk to become a loss. Threats consist of natural phenomena such as tornadoes and earthquakes and man-made incidents such as bomb threats, disgruntled employees, and power failures.
- Threat Vector** ➤ Information about a particular source of harm including where it originates and what path it takes to reach the protected asset.
- Throughput Rate** ➤ Unit for measuring the rate of information arriving at, and possibly passing through, a particular point in a network system.
- Token Bus** ➤ LAN architecture using token passing access over a bus topology. This LAN architecture is the basis for the IEEE 802.4 LAN specification.
- Token Frame** ➤ that contains control information. Possession of the token allows a network device to transmit data onto the network.
- Token Passing** ➤ A MAC method where stations may only transmit when they are in possession of a special bit sequence (token) passed from station to station.
- Token Ring** ➤ A ring topology network that uses token passing for MAC.
- Top-Down Approach** ➤ A way of designing a system starting with the big picture, by analyzing requirements, developing an architecture, and strategizing, as opposed to taking a bottom-up approach in which designs are based on technical product capabilities.
- Topology** ➤ 1. The arrangement of computing devices in a network. 2. A term describing such an arrangement.
- Tracer** ➤ A debugging technique, which shows the changes in selected variables during the execution of a program
- Transaction Log Back-Ups** ➤ Special database backups that contain a sequential record of all data modifications that have occurred within a database.
- Transceiver** ➤ 1. In Ethernet, an electronic device that transforms signals between a node's internal circuitry and the Ethernet signals and also detects collisions. 2. Any device that can simultaneously transmit and receive.
- Transfer Rate** ➤ The rate at which data is transferred from one device to another, usually expressed in bit per second or in bytes per second.
- Transitive Security** ➤ See Equivalent Security.

- Transport Layer** ➤ The layer of the OSI 7-Layer Model that is concerned with management of the data flow between source and destination.
- Trap Door** ➤ See Back Door.
- Trojan Horse** ➤ An apparently useful and innocent program containing additional hidden code that allows the unauthorized collection, exploitation, falsification, or destruction of data. A Trojan horse is often received from a familiar e-mail address or URL or in the form of a familiar attachment.
- Trustworthy** ➤ Having reliable, appropriate, and validated levels of security.
- UDP** ➤ User Datagram protocol.
- Unicast** ➤ A type of network packet traffic that is destined for one host only. See also Broadcast.
- Uninterruptible Power Supply (UPS)** ➤ A backup power supply with enough power to allow a safe and orderly shutdown of the central processing unit should there be a disruption or shutdown of electricity.
- Unit Testing** ➤ The most fundamental testing technique, where each program segment is separately tested
- Unix** ➤ A 32-bit multi-tasking, multi-user operating system; originally developed by Bell Labs
- User Interface** ➤ The collection of display symbols and other sensory stimuli made by a computer that present information to a human and the collection of physical action that a human can take to present data to a computer.
- Utility Software** ➤ Systems software that is useful in performing specific command sequences and routines to query on system activities or to achieve enhanced effectiveness and efficiency of systems functions.
- UTP** ➤ Unshielded twisted pair wiring.
- Vaporware** ➤ A computer program that has been publicly announced but is not shipped.
- Variant** ➤ A threat that is slightly modified to escape detection or that has slightly different behavior.
- Vines** ➤ A Network Operating System developed by Banyan.
- Virtual Private Network (VPN)** ➤ A network connection that traverses an untrusted network and that has two properties: end-to-end network connectivity (hence the term virtual) and confidentiality of data, usually provided by encryption (hence the term private).

Glossary

- Virus** ➤ A self-replicating program that uses other host files or code to replicate with a capability to harm the victim system. See also Appending Virus, Boot Virus, Macro Virus, Memory-Resident Virus, Multipartite Virus, Nonresident Virus, Overwriting Virus, Parasitic Virus, Prepending Virus and Stealth virus.
- VLAN (Virtual Local Area Network)** ➤ A logical grouping of two or more nodes that are not necessarily on the same physical network segment but that share the same IP network number. This is often associated with switched Ethernet.
- Voice Recovery** ➤ The restoration of an organization's voice communications system.
- Vulnerability** ➤ A characteristic that leads to exposure, and that may be exploited by a threat to cause harm. Vulnerabilities are most commonly a result of a software flaw or misconfiguration. See also Threat.
- WAN** ➤ Wide Area Network. A network that is created between and among devices separated by large distances
- Warm Site** ➤ An alternate processing site which is only partially equipped (as compared to Hot Site, which is fully equipped).
- Wave** ➤ The phenomenon that occurs when a physical medium is host to a measurable condition that varies in intensity, frequency or velocity with time.
- Weak Security** ➤ Security controls that are significantly less than completely effective. See also Strong Security.
- Well-Known Ports** ➤ Network ports from 0 to 1,023 assigned by the Internet Assigned Numbers Authority (www.iana.org) for commonly used network services and applications.
- White Box Approach** ➤ An auditing approach in which the auditor uses the computerized environment for achieving his audit objectives. In this approach, the auditor may review the source code, run audit tools and apply other computer aided auditing techniques.
- White Box Testing** ➤ This is a testing approach that uses knowledge of the program or module's underlying implementation to verify its expected behaviour.
- WLAN** ➤ A wireless LAN.
- Wireless** ➤ A System that provides communication without the use of wires.
- Wiring Closet** ➤ In wiring for telephone or data systems, any location from which the communication wires emanate, usually enclosed.

- Workgroup** ➤ A group of networked computer users who frequently communicate with each other and share common devices.
- Workstations** ➤ Special purpose machines designed for specific purpose such as CAD/CAM or graphics applications.
- Worm** ➤ A computer program that uses its own coding to replicate, unlike a computer virus that relies on other host files for replication. See also Virus.
- XWindows** ➤ A way of operating remote systems. The window allows the user to control and application remotely and view the application's output.
- X.25** ➤ A packet switching network.
- X.400** ➤ An OSI standard for a group of store and forward message handling services.
- X.500** ➤ Directory Services for OSI provides consistent data storage, retrieval and management for information about all network objects.
- Zombie** ➤ A Trojan horse program that infects host computer systems and awaits a command from a remote hacker to initiate a coordinated attack on another host. See also Trojan horse.
- Zones Of Trust** ➤ Different regions of networks and computer systems that have different levels of trust—some computer systems or networks must be trusted completely, some are trusted incompletely, and some are completely untrusted.

