CHAPTER 8

INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

- SA 315/330
  - AAS-29 was issued by ICAI: Establishing procedures to be followed when audit related accounting is carried out in a computer information system environment.
  - Effective from 1-4-2008, AAS-29 standard withdrawn pursuant to introduction of SA 315 & SA 330

- SA 315
  - Identifying & Assessing Risk of material misstatement through understanding the entity & its environments.
  - Relevant Extract: "the information system including
    - The related business processes,
    - relevant to financial Reporting &
    - Communications."
  - Identifying the risk of material misstatement
    - Significant risk
    - Material weakness

- SA 330: AUDITOR'S RESPONSE TO ASSESSED RISK
  - This standard on Auditing deals with the auditor's **RESPONSIBILITY TO DESIGN AND IMPLEMENT RESPONSES** to the risk of material misstatement identified & assessed by the auditor in accordance with SA 315.
  - Talks about issues like
    - Test of controls,
    - Nature & Extent of such test,
    - Timing there of
    - Evaluating the operating Effectiveness of controls substantive procedures,
    - Evaluating sufficiency & Appropriateness of Audit evidence
    - Documentation, etc.

- ISACA'S AUDIT STANDARDS, GUIDELINES, TOOLS & TECHNIQUES (PROCEDURES)
  - The IT Audit & Assurance standards are meat
    A. To inform the professionals of **THE MINIMUM LEVEL OF ACCEPTABLE PERFORMANCE REQUIRED** discharging their professional responsibility.
    B. Inform management & other stakeholders of the profession's expectations concern the work of its members.
  - Standards: Mandatory requirements for IT Audit & Assurance (currently there are 16 Standards)

- Guidelines: Provide guidance & Additional information on how to comply with IT Audit & assurance Standards. It is not mandatory. Currently 45 guidelines (19 being withdrawn)
- Tools & Techniques: They provide examples of procedures that can be followed during audit. It is not mandatory, but provides additional information. Currently there arte 11 tools & techniques.

⇨ ISO 27001 INFORMATION SECURITY MANAGEMENT STANDARD

- This standard pertains to the information security management. The various requirements of information security system have been stated below.
- General:
  Organization shall ESTABLISH AND MAINTAIN DOCUMENTED ISMS ADDRESSING
  - ASSETS TO BE PROTECTED,
  - ORGANIZATIONS APPROACH TO RISK MANAGEMENT,
  - CONTROL OBJECTIVES AND CONTROL, AND
  - DEGREE OF ASSURANCE REQUIRED.

When an organization is audited for the effective implementation of ISO 27001 Information Security Management System, What are to be verified under:
1. Establishing Management Framework?
2. Implementation?
3. Documentation? (M'09 – 10 Marks & M'11 – 08 Marks)

- Establishing Management Framework:
  This would include
  - Define information security policy;
  - Define scope of ISMS including functional, asset, technical, and locational boundaries;
  - Make appropriate risk assessment;
  - Identify areas of risk to be managed and degree of assurance required;
  - Select appropriate controls;
  - Prepare Statement of Applicability
- Implementation:
  The selected control objective & controls shall be implemented effectively by the organization.
- Documentation: The documentation shall consist of evidence of action undertaken under establishment of the following
  - Management control
  - Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
  - Procedure adopted to implement control under Implementation clause
  - ISMS management procedure
  - Document Control: The issues focused under this clause would be
    - Ready availability
    - Periodic review
    - Maintain version control;
    - Withdrawal when obsolete
    - Preservation for legal purpose
  - Records: The issues involved in record maintenance are as follows:
    - Maintain to evidence compliance to Part 2 of BS7799.;

- Procedure for identifying, maintaining, retaining, and disposing of such evidence;
- Records to be legible, identifiable and traceable to activity involved.
- Storage to augment retrieval, and protection against damage.

⇨ AREAS OF FOCUS OF ISMS

There are ten areas of focus of ISMS. These are described in the following paragraphs:

1. SECURITY POLICY:
   - This activity involves a thorough understanding of **THE ORGANIZATION BUSINESS GOALS** and its dependence on **INFORMATION SECURITY**.
   - It should reflect the needs of the **ACTUAL USERS.**
   - It should be implementable, easy to understand and must balance the level of protection with productivity.
   - The policy should cover:
     - a **DEFINITION** of information security,
     - a statement of **MANAGEMENT INTENTION** supporting the goals and principles of information security,
     - allocation of **RESPONSIBILITIES**,
     - an **EXPLANATION** of specific applicable proprietary and general, principles, standards and compliance requirements,
     - an **EXPLANATION OF THE PROCESS** for reporting of suspected security incidents,
     - a defined review process for maintaining the **POLICY DOCUMENT**,
     - means for assessing the effectiveness of the policy **EMBRACING COST** and **TECHNOLOGICAL CHANGES**, and
     - Nomination of the **POLICY OWNER**.
   - The detailed control and objectives are as follows:
     - **INFORMATION SECURITY POLICY**: To provide management direction and support for information security,
     - **INFORMATION SYSTEM INFRASTRUCTURE**: To manage information security within the organization,
     - **SECURITY OF 3RD PARTY ACCESS**: To maintain the security of organizational information processing facilities and information assets accessed by third parties, and
     - **OUTSOURCING:** To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

2. ORGANIZATIONAL SECURITY:
   - A management framework needs to be established to '**INITIATE, IMPLEMENT AND CONTROL** '**INFORMATION SECURITY** within the organization.
   - This needs proper procedures for approval of the information security policy, assigning of the **SECURITY ROLES AND COORDINATION** of security across the organization.
   - The detailed control and objectives are as follows :
     - **INFORMATION SYSTEM INFRASTRUCTURE** : To manage information security within the organization
     - **SECURITY OF 3RD PARTY ACCESS**: To maintain the security of organizational information processing facilities and information assets accessed by third parties
     - **Outsourcing**: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

3. ASSET CLASSIFICATION AND CONTROL (M'09- 5 Marks) :
   - Manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services.
   - These information assets need to be **CLASSIFIED TO INDICATE THE DEGREE OF PROTECTION**.
   - The classification should result into **APPROPRIATE INFORMATION LABELING** to indicate whether it is sensitive or critical and what procedure, which is appropriate for copy, store, and transmit or destruction of the information asset.
   - An Information Asset Register (IAR) should be created with the details of every information asset within the organization.
   - For example:
     - Databases
     - Personnel records
     - Scale models
     - Prototypes
     - Test samples
     - Contracts
     - Software licenses
     - Publicity material
   - The Information Asset Register (IAR) should also describe **WHO IS RESPONSIBLE** for each information asset and whether there is any special requirement for confidentiality, integrity or availability.
   - For administrative convenience, **SEPARATE REGISTER** may be maintained under the subject head of IAR
   - For e.g.
     - 'Media register' will detail the stock of software and its licenses.
     - 'Contracts Register' will contain the contracts signed and thus other details

     The value of each asset can then be determined to ensure appropriate security is in place.
   - The detailed **CONTROL AND OBJECTIVES** thereof are as follows:
     - **ACCOUNTABILITY FOR ASSETS**: To maintain appropriate protection of organizational assets
     - **INFORMATION CLASSIFICATION**: To ensure that information assets receive an appropriate level of protection.

4. PERSONNEL SECURITY:
   - Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities.
   - Various **PROACTIVE MEASURES** that should be taken are,
     - To make personnel screening policies, confidentiality agreements, terms and conditions of employment,
     - Information security education and training.
   - Appropriate personnel security ensures that :
     - Employment **Contracts** and staff **handbooks** have agreed, clear wording
     - Ancillary workers, temporary staff, contractors and **third parties** are covered
     - Anyone else with legitimate **access to business** information or systems is covered
   - It must deal with rights as well as responsibilities, for example:
     - Access to personal files under the Data Protection Act
     - Proper use of equipment as covered by the Computer Misuse Act (In India that would be Information Technology Act 2000)

- The detailed control and objectives thereof are as follows:
  - **SECURITY IN JOB DEFINITION AND RESOURCING**: To reduce the risks of human error, theft, fraud, or misuse of facilities
  - **USER TRAINING**: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in course of their normal work
  - **RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS**: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

5. PHYSICAL AND ENVIRONMENTAL SECURITY (N'09- 5 Marks):
   - Designing a secure physical environment **TO PREVENT UNAUTHORIZED ACCESS, DAMAGE AND INTERFERENCE** to business premises and information is important.
   - **COST EFFECTIVE DESIGN AND CONSTANT MONITORING** are two key aspects to maintain adequate physical security control. E.g. Physical entry control, physical access control, fire safety, etc.
   - **ENSURE PROPER MAINTENANCE** of computer server room, paper records, supporting equipment and main services.
   - The detailed control and objectives thereof are as follows:
     - **SECURE AREAS**: To prevent unauthorized access, damage and interference to business premises and information
     - **EQUIPMENT SECURITY**: To prevent loss, damage or compromise of assets and interruption to business activities
     - **GENERAL CONTROLS**: To prevent compromise or theft of information and information processing facilities

6. COMMUNICATIONS AND OPERATIONS MANAGEMENT:
   - Properly **DOCUMENTED PROCEDURES** for the management and operation of all information processing facilities should be established.
   - This includes detailed **OPERATING INSTRUCTIONS AND INCIDENT RESPONSE PROCEDURES.**
   - Network:
     - Management requires a range of controls to achieve and maintain security in computer networks.
     - This also includes establishing procedures for remote equipment including equipment in user areas.
     - Special controls should be established to ensure
       - The confidentiality and integrity of data passing over public networks.
       - Availability of the network services.
   - Exchange
     - Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation.
     - There should be proper information and software exchange agreements, the media in transit.
   - Electronic commerce
     - E-commerce involves electronic data interchange, electronic mail and online transactions across public networks such as Internet.
     - Controls should be applied to protect electronic commerce from such threats.

- The detailed **CONTROL AND OBJECTIVES** thereof are as follows:
  - Operational procedures and responsibilities: To ensure correct and secure operation of information processing facility
  - System planning and acceptance: To minimize risks of system failure
  - Protection against malicious software: To protect the integrity of software and info
  - Housekeeping: To maintain the integrity and availability of information processing and communication services
  - Network Management: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
  - Media handling and security : Prevent damage to assets and interruptions to business activity
  - Exchanges of information and software: To prevent loss, modification or misuse of information exchanged between organizations

7. ACCESS CONTROL:
   - Access to information and business processes should be controlled on the business and security requirements.
   - This will include
     - defining access control policy and rules,
     - user access management,
     - user registration,
     - privilege management,
     - user password use and management,
     - review of user access rights, network access controls,
     - enforcing path from user terminal to computer,
     - user authentication,
     - node authentication,
     - segregation of networks,
     - network connection control,
     - network routing control,
     - operating system access control,
     - user identification and authentication,
     - use of system utilities,
     - application access control,
     - monitoring system access and
     - Use and ensuring information security when using mobile computing and tele-working facilities.
   - The detailed control and objectives thereof are as follows:
     - Business requirement for access control: To control access to information
     - User access management : To prevent unauthorized access to info systems
     - User responsibilities : To prevent unauthorized user access
     - Network access control : Protection of networked services
     - Operating system access control : To prevent unauthorized computer access
     - Application Access Control : To prevent unauthorized access to information held in information systems
     - Monitoring System Access and use : To detect unauthorized activities
     - Mobile Computing and teleworking : To ensure information security when using mobile computing & teleworking facilities

8. SYSTEMS DEVELOPMENT AND MAINTENANCE:

- Security requirements should be **IDENTIFIED AND AGREED PRIOR TO THE DEVELOPMENT** of information systems.
- This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data processing, data storage and retrieval and data output.
- There should be a defined policy on the use of such controls, which may involve
  - encryption,
  - digital signature,
  - use of digital certificates,
  - protection of cryptographic keys and
  - Standards to be used for cryptography.
- A strict **CHANGE CONTROL PROCEDURE** should be in place to facilitate **TRACKING** of changes.
- Special precaution must be taken to ensure that no
  - Covert channels,
  - Back doors or
  - Trojans are left in the application system for later exploitation.
- The detailed control and objectives thereof are as follows:
  - Security requirements of system : To ensure that security is built into information systems
  - Security in application systems : To prevent loss, modification or misuse of user data in application system
  - Cryptographic Controls : To protect the confidentiality, authenticity or integrity of information
  - Security of system files : To ensure that IT projects and support activities are conducted in a secure manner
  - Security in development and support process : To maintain the security of application system software and information

9. BUSINESS CONTINUITY MANAGEMENT:

- A business continuity management process should be
  - DESIGNED,
  - IMPLEMENTED AND
  - PERIODICALLY TESTED

  TO REDUCE THE DISRUPTION CAUSED BY DISASTERS AND SECURITY FAILURES.
- This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan.
- The plan needs to be periodically tested, maintained and re-assessed based on changing circumstances
- There is only one control, which is described here along with its objectives:
  - Aspects of business continuity management: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters

10. COMPLIANCE :

- It is essential that strict adherence is observed to
  - the provision of national and international IT laws,
  - pertaining to Intellectual Property Rights (IPR),
  - software copyrights,
  - safeguarding of organizational records,

- ✳ data protection and privacy of personal information,
- ✳ prevention of misuse of information processing facilities,
- ✳ regulation of cryptographic controls and
- ✳ Collection of evidence

☞ The detailed control and objectives thereof are as follows:

- ✳ **COMPLIANCE WITH LEGAL REQUIREMENTS** : To avoid breaches of any
  - criminal and civil law,
  - and statutory,
  - regulatory, or
  - contractual obligations, and
  - of any security requirements
- ✳ **REVIEW OF SECURITY POLICY AND TECHNICAL COMPLIANCE** : To ensure compliance of systems with organizational security policies and standards
- ✳ **SYSTEM AUDIT CONSIDERATION** : To maximize the effectiveness, and to minimize interference to/from the system audit process

⇨ CAPABILITY MATURITY MODEL (CMM)

☞ The capability Maturity Model for software provides software organizations with GUIDANCE on

- ✳ How to gain control of their processes for developing & maintaining software &
- ✳ How to evolve toward a culture of software engineering & Management excellence.

How will you define a software process? What do you mean by capability, performance and maturity? (N'10- 4 Marks)

☞ <u>Software Process:</u>

- ➢ A software process can be defined as
  - ✳ A SET OF ACTIVITIES, METHODS, PRACTICES, AND TRANSFORMATIONS
  - ✳ THAT PEOPLE USE TO DEVELOP AND
  - ✳ MAINTAIN SOFTWARE AND
  - ✳ THE ASSOCIATED PRODUCTS
- ➢ e.g., project plans, design documents, code, test cases, and user manuals

☞ <u>Software process capability:</u>

- ➢ Software process capability describes **THE RANGE OF EXPECTED RESULTS** that can be achieved by following a software process.
- ➢ It helps predicting the most likely outcomes to be expected from the next software project the organization undertakes.

☞ <u>Software process performance:</u>

- ➢ Software process performance represents the **ACTUAL RESULTS** achieved by following a software process.
- ➢ It focuses on the results achieved.

☞ <u>Software process maturity:</u>

- ➢ Software process maturity is the **EXTENT TO WHICH A SPECIFIC PROCESS IS EXPLICITLY DEFINED, MANAGED, MEASURED, CONTROLLED, AND EFFECTIVE**.
- ➢ It institutionalizes its software process via policies, standards, and organizational

structures.

- WHAT IS CMM?
  - ✳ High quality software organizations are different from low quality organization.
  - ✳ CMM tires to capture & describe these differences.
  - ✳ CMM strives to create software development organizations that are “mature” or more mature than before applying of Software process maturity.
  - ✳ It describes 5 level of software process maturity.
  - ✳ It includes lots of details about each level we will look at some of it.

What do you understand software process maturity? Discuss 5 level of software process maturity of capability maturity model (CMM). (N’08- 10 Marks) Or Write a short Note on Capability Maturity model (N’11- 4 Marks)

LEVEL	CHARACTERISTICS
Level 1 –The initial Level	✳ No stable environment for developing and maintaining software. ✳ Difficulty making commitments that the staff can meet with an orderly engineering process, resulting in a series of crises. ✳ During a crisis, projects typically abandon planned procedures and revert to coding and testing. ✳ Capability is characteristic of the individual, not of organization ✳ But if some one leaves the project, it difficult to handle the crisis and changeling tasks.
Level 2 the Repeatable Level	✳ At the Repeatable Level, policies for managing a software project and procedures to implement those policies are established. ✳ Planning and managing new projects is based on experience with similar projects. ✳ An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. ✳ This Level makes organizations have installed basic software management controls. ✳ Software project standards are defined. ✳ The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
Level 3 The Define Level	✳ At this level documentation for development and maintenance is prepared. ✳ This standard process is referred to throughout the CMM as the organization's standard software process, to help the software managers and technical staff performs more effectively. ✳ A group of experts standardize the process. ✳ An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned roles. ✳ This process capability is based on a common, organization-wide

	understanding of the activities, roles, and responsibilities in a defined software process.
Level 4 The Managed Level	✳ At the Managed Level, the organization sets quantitative quality goals for both software products and processes. ✳ Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. ✳ An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes. ✳ This level of process capability allows an organization to predict trends in process and product quality within the quantitative bounds of these limits. ✳ Because the process is both stable and measured, when some exceptional circumstance occurs, the "special cause" of the variation can be identified and addressed. ✳ Software products are of predictably high quality.
Level 5 The optimizing Level	✳ The entire organization is focused on continuous process improvement. ✳ The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. ✳ Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. ✳ In short, the cost of development is cut; best engineering practices are developed and used. ✳ Continues improvement is done. ✳ Technology and process improvements are planned and managed as ordinary business activities.

⇨ COBIT

- ☞ What COBIT is not!!
  - ✳ Audit software
  - ✳ An IT Audit Plan
  - ✳ An IT Internal Audit work Program
  - ✳ An It Audit Testing Plan
  - ✳ Guide on How to Audit it.
- ☞ Then what is COBIT?
  - ✳ **It is THE CONTROL OBJECTIVE FOR INFORMATION AND RELATED TECHNOLOGY**
  - ✳ A methodology consisting of standard and controls created to assist it professional in the implementation review, administration & monitoring of it environment.
  - ✳ The COBIT executive summary and framework were released in December 1995, control objective in April 1996, and audit guidelines followed in September 1996.
  - ✳ A tool that for IT professional that has linked information technology & control

Practices.

- COBIT consolidates & harmonizes standards from prominent global sources in to a critical resources for management, control professional and Auditors.
- COBIT represents
  - A control framework,
  - A set of generally accepted control objective &
  - The COBIT Audit guidelines.
- COBIT is based on the philosophy that IT resources need be managed by a set of naturally grouped process in order to provide the pertinent & reliable information an organization needs to achieve its objective.
- COBIT is business process oriented provide the business process owners with a framework, which should be enable them to controlled the different activities underlying it development.

☞ What is the purpose of COBIT?

- To provide management & business process owner with an information technology (IT) governable model that helps in understanding & managing the risk associated with it.
- COBIT helps bridge gap between business risk, control needs & technical issues presenting the controls through one vehicle.
- It is a control model to meet the need of IT Governance and ensure the integrity of information and information system.

☞ Components of COBIT

The 4 domains of COBIT

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

- <u>Plan and Organize</u>

  - The Plan and Organize domain covers the **USE OF INFORMATION & TECHNOLOGY** and how best it can be used in a company to help achieve the company's goals and objectives.
  - It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT.
  - The following table lists the IT processes contained in the Planning and Organization domain.

IT PROCESSES Plan and Organize	
PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization and
PO5	Manage the IT Investment

PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects

✳ Acquire and Implement

- The Acquire and Implement domain covers **IDENTIFYING IT REQUIREMENTS, ACQUIRING THE TECHNOLOGY, AND IMPLEMENTING** it within the company's current business processes.
- This domain also addresses the **DEVELOPMENT OF A MAINTENANCE PLAN** that a company should adopt in order to prolong the life of an IT system and its components.
- The following table lists the IT processes contained in the Acquire and Implement domain.

IT PROCESSES Acquire and Implement

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredit Solutions and Changes

✳ Deliver and Support

- The Deliver and Support domain focuses on the **DELIVERY ASPECTS OF THE INFORMATION TECHNOLOGY.**
- It covers areas such as the **EXECUTION** of the applications within the IT system and its results as well as the support processes that enable the effective and efficient execution of these IT systems.
- These support processes include security issues and training.
- The following table lists the IT processes contained in the Deliver and Support domain.

IT PROCESSES Deliver and Support

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents

DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

✳ Monitor and Evaluate

- This domain helps assessee whether **THE CURRENT SYSTEM STILL MEETS THE OBJECTIVES** for which it was designed and the controls needed to comply with regulatory requirement.
- Monitoring also covers the issue of an **INDEPENDENT ASSESSMENT** of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors.
- The following table lists the IT processes contained in the Monitor and Evaluate domain.

IT PROCESSES Monitor and Evaluate

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

⇨ COCO OR GUIDANCE ON CONTROL REOPRT

- The "Guidance on Control" report, known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants.
- CoCo is "guidance," meaning that
  - ✳ It is not intended as "**PRESCRIPTIVE MINIMUM REQUIREMENTS**"
  - ✳ but rather as "**USEFUL IN MAKING JUDGMENTS**"
  - ✳ About "**DESIGNING, ASSESSING AND REPORTING ON THE CONTROL SYSTEMS OF ORGANIZATIONS**."
- CoCo can be said to be a concise superset of COSO.
- It uses three categories of objectives:
  - ✳ effectiveness and efficiency of operations
  - ✳ reliability of financial reporting
  - ✳ compliance with applicable laws and regulations
- CoCo states that the "essence of control is purpose, capability, commitment, and monitoring and learning,"
- These form a cycle that continues endlessly if an organization is to continue to improve.
- Four important concepts about "control" are as follows:
  - ✳ Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
  - ✳ People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives.
  - ✳ Organizations are constantly interacting and adapting.
  - ✳ Control can be expected to provide only **REASONABLE ASSURANCE, NOT ABSOLUTE ASSURANCE.**

⇨ ITIL (IT INFRASTRUCTURE LIBRARY)

- ITIL is originated from the UK
- UK Government was not satisfied with quality of services from internal and external IT Companies.
- CCTA (Central Computer and Telecommunication Agency) was instructed to develop a standard approach for efficient and effective delivery of IT Services.
- Collection of "Best Practices".
- The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific 'practice' within IT management.
- After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books.
- The eight ITIL books and their disciplines are: The IT Service Management sets relating to:

1. Service Delivery
2. Service Support

Other operational guidance relating to:

3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management

   To assist with the implementation of ITIL practices a further book was published providing guidance on implementation (mainly of Service Management)

8. Planning to Implement Service Management

- **Details of the ITIL Framework**

a) **SERVICE SUPPORT**

- ITIL discipline is focused on the User of the ICT services and is primarily concerned with ensuring that they have access to the appropriate services to support the business functions.
- The service desk will try to resolve it, if there is a direct solution or will create an incident.
- Incidents initiate a chain of processes:
  - Incident Management,
  - Problem Management,
  - Change Management,
  - Release Management and
  - Configuration Management

b) **PROBLEM MANAGEMENT**

- The goal is to resolve the root cause of incidents and thus to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.
- A `problem' is an unknown underlying cause of one or more incidents, and a `known error' is a problem that is successfully diagnosed and for which a work-around has been

identified

c) **CONFIGURATION MANAGEMENT**

- Configuration Management is a process that tracks all of the individual Configuration Items (CI) in a system.
- A system may be as simple as a single server, or as complex as the entire IT department.
- Configuration Management includes:
  - Creating a parts list of every CI (hardware or software) in the system.
  - Defining the relationship of CIs in the system
  - Tracking of the status of each CI, both its current status and its history.
  - Tracking all Requests for Change to the system.
  - Verifying and ensuring that the CI parts list is complete and correct.
- There are five basic activities in configuration management:
  - Planning
  - Identification
  - Control
  - Status accounting
  - Verification and Audit

d) **RELEASE MANAGEMENT**

- Release Management is used for
  - platform-independent and
  - automated distribution of software and hardware,
  - Including license controls across the entire IT infrastructure.
- Proper **SOFTWARE AND HARDWARE CONTROL** ensures the availability of licensed, tested, and version certified software and hardware, which will function correctly and respectively with the available hardware.
- **QUALITY CONTROL** during the development and implementation of new hardware and software is also the responsibility of Release Management.
- This guarantees that all software can be conceptually optimized to meet the demands of the business processes.
- The goals of release management are:
  - Plan to rollout of software
  - Design and implement procedures for the distribution and installation of changes to IT systems
  - Effectively communicate and manage expectations of the customer during the planning and rollout of new releases
  - Control the distribution and installation of changes to IT systems.

e) **SERVICE DELIVERY**

- The Service Delivery discipline is primarily concerned with the proactive and forward-looking services that the business requires of its ICT provider in order to provide adequate support to the business users.
- It is focused on the business as the Customer of the ICT services (compare with: Service Support).
- The discipline consists of the following processes, explained in subsections below:
  - Service Level Management
  - Capacity Management
  - IT Service Continuity Management
  - Availability Management

- Financial Management

f) **SERVICE LEVEL MANAGEMENT**

- Service Level Management provides for continual identification, monitoring and review of the levels of IT services specified in the Service Level Agreements (SLAs).
- Service Level Management ensures that arrangements are in place with internal IT support providers and external suppliers in the form of Operational Level Agreements (OLAs) and Underpinning Contracts (UpCs).
- The process involves assessing the impact of change upon service quality and SLAs.

g) **CAPACITY MANAGEMENT**

- Capacity Management supports the **OPTIMUM AND COST EFFECTIVE PROVISION** of IT services by helping organizations match their IT resources to the business demands.
- The high-level activities are
  - Application Sizing,
  - Workload Management,
  - Demand Management,
  - Modeling,
  - Capacity Planning,
  - Resource Management, and
  - Performance Management.

h) **SECURITY MANAGEMENT**

- ITIL Security Management is based on the code of practice for information security management also known as ISO/IEC 17799.
- A basic concept of the Security Management is the information security.
- The primary goal of information security is to guarantee the safety of the information by the confidentiality, integrity and availability.

i) **ICT INFRASTRUCTURE MANAGEMENT**

ICT Infrastructure Management processes recommend best practice for

- Requirements analysis,
- Planning,
- Design,
- Deployment and ongoing operations of management and
- Technical support of an ICT Infrastructure.

j) **THE BUSINESS PERSPECTIVE**

- The Business Perspective refers to best practices aimed to solving issues encountered in understanding and improving IT service.
- These issues are:
  - Business Continuity Management
  - Surviving Change
  - Transformation of business practices via IT.
  - Partnerships and outsourcing.

k) **APPLICATION MANAGEMENT**

ITIL Application Management set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects.

l) **SOFTWARE ASSET MANAGEMENT**

Good Software Asset Management achieved through Best Practice enables organizations to save money through effective policies and procedures which are continuously reviewed and

improved.

⇨ SYSTRUST & WEBTRUST (N'10- 4 Marks)

- ☞ SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria.
- ☞ SysTrust engagements are designed for **THE PROVISION OR ADVISORY SERVICES OR ASSURANCE ON THE RELIABILITY OF A SYSTEM**.
- ☞ WebTrust engagements relate to **ASSURANCE OR ADVISORY SERVICES ON AN ORGANIZATION'S SYSTEM RELATED TO E-COMMERCE**.
- ☞ Only certified public accountants (CPAs) may provide the assurance services of Trust Services that result in the expression of a Trust Services, WebTrust, or SysTrust opinion, and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.
- ☞ Principle
  - ✳ Security: The system is protected against unauthorized access (both physical and logical).
  - ✳ Availability: The system is available for operation and use as committed or agreed.
  - ✳ Processing integrity: System processing is complete, accurate, timely, and authorized.
  - ✳ Online privacy: Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
  - ✳ Confidentiality: Information designated as confidential is protected as committed or agreed.

⇨ HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress in 1996.

- ☞ Title I of HIPAA protects **HEALTH INSURANCE COVERAGE** for workers and their families when they change or lose their jobs

- ☞ Title II of HIPAA, the **ADMINISTRATIVE SIMPLIFICATION** (AS) provisions, requires the following:
  - ✳ Establishment of **NATIONAL STANDARDS** for electronic health care transactions and **NATIONAL IDENTIFIERS** for providers, health insurance plans, and employers.
  - ✳ The AS provisions also address the security and **PRIVACY OF HEALTH DATA**.
  - ✳ The standards are meant to improve the **EFFICIENCY AND EFFECTIVENESS OF THE NATION'S HEALTH CARE SYSTEM** by encouraging the widespread use of electronic data interchange in the US health care system.
- ☞ What is of interest here is the Security Rule issued under the Act.

THE SECURITY RULE (APT)

- ☞ The Security lays out three types of security safeguards required for compliance:
  - ✳ Administrative,
  - ✳ Physical, and
  - ✳ Technical.
- ☞ For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications.
  - ✳ **REQUIRED SPECIFICATIONS** must be adopted and administered as dictated by the Rule.
  - ✳ **ADDRESSABLE SPECIFICATIONS** are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable

specifications.

☞ The standards and specifications are as follows:

a) **ADMINISTRATIVE SAFEGUARDS:**

Policies and procedures designed to clearly show how the entity will **COMPLY** with the act

- ✳ Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
- ✳ The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
- ✳ Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI).
- ✳ The procedures must address access authorization, establishment, modification, and termination.
- ✳ Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.
- ✳ Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements.
- ✳ A contingency plan should be in place for responding to emergencies.
- ✳ Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- ✳ Internal audits helps in identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- ✳ Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

b) **PHYSICAL SAFEGUARDS**

Controlling physical access to protect against inappropriate access to protected data

- ✳ Controls must govern the introduction and removal of hardware and software from the network.
- ✳ Access to equipment containing health information should be carefully controlled and monitored.
- ✳ Access to hardware and software must be limited to properly authorized individuals.
- ✳ Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- ✳ Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- ✳ If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

c) **TECHNICAL SAFEGUARDS**

Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

- ✳ Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- ✳ Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- ✳ Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
- ✳ Covered entities must also authenticate entities; it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone call-back, and token systems.
- ✳ Documentation of HIPAA practices available to the government to determine compliance.
- ✳ Information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
- ✳ Documented risk analysis and risk management programs are required.

⇨ SAS 70 STATEMENT OF AUDITING STANDARDS FOR SERVICE ORGANISATIONS

What do you think separate standard (SAS 70) is useful for auditing a service organization especially with respect to examination of general controls over information technology and related processes? (N'10 – 4 Marks)

- ☞ ORIGIN: 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).
- ☞ WHAT: A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an **IN-DEPTH AUDIT** of their control activities, which generally include controls over information technology and related processes.
- ☞ WHY: 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**.
- ☞ IMPORTANCE OF SAS 70
  - ✳ SAS 70 No. is **AUTHORITATIVE GUIDANCE** that allows service organizations to **DISCLOSE** their control activities and processes to their customers and their customers' auditors in a **UNIFORM REPORTING FORMAT**.
  - ✳ A SAS 70 examination signifies that a service organization has had its control objectives and control activities **EXAMINED BY AN INDEPENDENT** accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.
  - ✳ SAS 70 provides **GUIDANCE** to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report.
  - ✳ SAS 70 is **NOT A PRE-DETERMINED** set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

- ✳ SAS No. 70 is generally applicable when an auditor ("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 centre's, Internet data centres, or other data processing service bureaus.

☞ SERVICE AUDITOR'S REPORTS (SAR):

What do you understand from Type I & Type II report from Service Auditor? (N'10- 4Marks)

- ✳ A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.
- ✳ There are two types of Service Auditor's Reports: Type I and Type II.

1. **A Type I report** describes the service organization's **DESCRIPTION OF CONTROLS AT A SPECIFIC POINT IN TIME** (e.g. June 30, 2003).
2. **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 MINIMUM SIX MONTH PERIOD** (e.g. January 1, 2003 to June 30, 2003).

- ✳ The contents of each type of report are described in the following table:

Report Contents	Type I Report	Type II Report
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Optional

- ✳ **Type I report:** the service auditor will express an opinion on
  - ✍ (1) whether the service organization's **DESCRIPTION** of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and
  - ✍ (2) Whether the controls were suitably designed to achieve specified control objectives.
- ✳ **Type II report**: the service auditor will express an opinion on
  - ✍ the same items noted above in a Type I report, and
  - ✍ (3) whether the controls that were **TESTED WERE OPERATING** with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

☞ BENEFITS TO THE SERVICE ORGANIZATION

- ✳ A Service Auditor's Report with an unqualified opinion **DIFFERENTIATES** the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities.
- ✳ A Service Auditor's Report also helps a service organization build **TRUST** with its user

organizations (i.e. customers).

- ✳ Without a current Service Auditor's Report, a service organization may have to entertain **MULTIPLE AUDIT REQUESTS FROM** its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources.
- ✳ A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of **OPPORTUNITIES FOR IMPROVEMENTS** in many operational areas.

☞ BENEFITS TO THE USER ORGANIZATION: User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information:

- ✳ Detailed **DESCRIPTION** of the service organization's controls and the effective of those control
- ✳ An **INDEPENDENT ASSESSMENT** of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).