ISCA REVISION

COMPILED BY: CA NIKUNJ S. SHAH

VERSION : 1

RELEASED ON: FRIDAY, 23RD JANUARY 2015

Note:

1. This material covers key points of all Chapters of Paper 6 – Information Systems Control And Audit of the Final CA examination conducted by ICAI.
2. This material is applicable to students appearing for **May 2015 examinations.**
3. The objective of this material is to enable students revise the subject effectively in short and limited time.
4. This material may be distributed freely.
5. For updates, check Files section at www.groups.yahoo.com/group/ISCAicai

I N D E X

CHAPTER 1: CONCEPTS OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEMS

There are three levels of managerial activity in an enterprise • Strategic Planning, • Management Control, and • Operational Control.	**Strategic planning** is defined as the process of deciding on 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.	The **primary objective of IT strategy** is to provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Alignment of the strategic IT plans with the business objectives is done by clearly communicating the objectives and associated accountabilities, identifying, structuring and integrating IT strategies with the business plans as required.	**Key Management Practices to align IT Strategy with Enterprise Strategy:** Understand enterprise direction Assess the current environment, capabilities and performance: Define the target IT capabilities Conduct a gap analysis Define the strategic plan and road map: Communicate the IT strategy and direction
Key management practices to evaluate 'whether business value is derived from IT': • Evaluate Value Optimization • Direct Value Optimization • Monitor Value Optimization **Key metrics for evaluation:** 1. % of IT services where expected benefits realized; 2. % of IT enabled investments	where claimed benefits met or exceeded 3. % of investment business cases with clearly defined & approved expected IT related costs & benefits; 4. Satisfaction survey of key stakeholders reg. transparency, understanding and accuracy of IT financial information.	**IT STEERING COMMITTEE** is a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives.	It is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

Key functions of IT Steering Committee include: • To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives; • To establish size and scope of IT function and sets priorities within the scope; • To review and approve major IT deployment projects in all their stages;	• To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.; • To review the status of IS plans and budgets and overall IT performance; • To review & approve standards, policies & procedures; • To make decisions on all key aspects of IT deployment and implementation;	• To facilitate implementation of IT security within enterprise; • To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and • To report to the Board of Directors on IT activities on a regular basis.	**IT strategy plan - Categories:** i. Enterprise Strategic Plan, ii. Information Systems Strategic Plan, iii. Information Systems Requirements Plan, and iv. Information Systems Applications and Facilities Plan.
i. Enterprise Strategic Plan: □ Determines the overall plan of the enterprise. □ Provides the overall charter under which all units in the enterprise, including the information systems function must operate. □ Prepared by top management □ Guides the long term development of the enterprise.	□ It includes: (a) a statement of mission, (b) a specification of strategic objectives, (c) an assessment of environmental and organization factors that affect the attainment of these objectives, (d) a statement of strategies for achieving the objectives, (e) a specification of constraints that apply, (f) a listing of priorities.	**ii. Information Systems Strategic Plan:** □ Focuses on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment. □ Some of the enablers of the IS Strategic plan are: • 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, and • Need for senior management buy-in, support and critical review.

iii. Information Systems Requirements Plan: □ Defines information system architecture for IS department. □ A clearly defined information architecture optimises the organization's the information systems. □ Key enablers: • Automated data repository and dictionary, • Data syntax rules, • Data ownership and criticality/security classification, • An information model representing the business, and • Enterprise information architectural standards.	**iv. Information Systems Applications & Facilities Plan.** - Is developed by IS Management on basis of the information systems architecture and its associated priorities. **This plan includes:** • Specific application systems to be developed and an associated time schedule, • Hardware and Software acquisition/development schedule, • Facilities required, and Organization changes required.	**RISK MANAGEMENT:** Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management thus involves identifying, measuring, and minimizing uncertain events affecting resources.	**Vulnerability** is the weakness in the system safeguards that exposes the system to threats. **Threat** is any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data and denial of services. **Exposure** is the extent of loss the organisation has to face when a risk materializes. **Attack** is a set of actions designed to compromise confidentiality, integrity, availability or any other desired feature of an information system.
Risk: Defined as potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset. **Countermeasure:** An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as countermeasure **Residual Risk:** Any risk still remaining after counter measures analysed & implemented.	**Risk Management Strategies** 1. **Tolerate / Accept risk:** Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.	2. **Terminate / Eliminate risk:** If risk is associated with the use of a particular technology, supplier, or vendor it can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.	3. **Transfer / Share risk:** Risk can be shared with trading partners and suppliers. e.g. outsourcing infrastructure management. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

4. **Treat / mitigate risk:** Suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects. 5. **Turn back:** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.	**GOVERNANCE** ➢ Derived from Greek verb 'Kubernan' meaning "to steer". ➢ Refers to all the means and mechanisms that will enable multiple stake-holders to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives.	**Enterprise Governance:** Set of responsibilities and practices exercised by the board and executive management with the goal of ➢ providing strategic direction, ➢ ensuring that objectives are achieved, ➢ ascertaining that risks are managed appropriately and ➢ verifying that the organization's resources are used responsibly.'	**Governance Dimensions** Governance has two dimensions • Conformance or Corporate Governance • Performance or Business Governance
Conformance or Corporate Governance Dimension: ➢ Has a historic view. ➢ Focuses on regulatory requirements. ➢ Covers issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance. ➢ Regulatory requirements and standards generally address this dimension ➢ Compliance is subject to assurance and / or audit.	**Performance or Business Governance Dimension:** ➢ Takes a forward looking view. ➢ Focuses on strategy and value creation ➢ Does not lend itself to a regime of standards and assurance ➢ No dedicated oversight mechanism (as comparable to the audit committee) and thus this critical area of strategy does not get the same dedicated attention as corporate governance.	**Corporate Governance:** • 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. • Refers to the structures and processes for the direction and control of companies. • Concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders.	**Good corporate governance requires:** • 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.

Best practices of corporate governance • Responsibility & Authority, Hierarchy • Interaction & Cooperation • Internal Controls • Monitoring Risk – Conflict of Interest • Compensation • Information flow	**IT GOVERNANCE** "IT governance is the system by which **IT activities** in a company or enterprise **are directed and controlled** to achieve business objectives with the ultimate objective of meeting stakeholder needs". Objective - to determine & cause desired behaviour and results to achieve strategic impact of IT.	**Subset of enterprise governance**, which ensures that implementation of IT meets all the stakeholder requirements including regulators and management. Overall objective of IT governance is very much similar to corporate governance but with the focus on IT. Inseparable relationship between corporate governance and IT governance	**Key practices to determine status of IT Governance :** • Who makes directing, controlling and executing decisions? • How the decisions are made? • What information is required to make the decisions? • What decision-making mechanisms are required? • How exceptions are handled? • How the governance results are monitored and improved?
Benefits of IT Governance • Increased value delivered through enterprise IT; • Increased user satisfaction with IT services; • Improved agility in supporting business needs; • Better cost performance of IT; • Improved management & mitigation of IT-related business risk;	• IT becoming an enabler for change rather than an inhibitor; • Improved transparency and understanding of IT's contribution to the business; • Improved compliance with relevant laws, regulations and policies; and • More optimal utilization of IT resources.	**GEIT -** Although the terms IT Governance and Governance of Enterprise IT (GEIT) are used inter-changeably, the term GEIT is more macro and broader in its scope of coverage. **GEIT:** **1**. puts in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives. **2.** Facilitates implementation of a framework of IS controls	**Benefits of GEIT:** • It provides a consistent approach integrated and aligned with the enterprise governance approach. • It ensures that IT-related decisions are made in line with enterprise's strategies & objectives. • It ensures that IT-related processes are overseen effectively and transparently. • It confirms compliance with legal and regulatory requirements. • It ensures that the governance requirements for board members are met.

ENTERPRISE RISKMANAGEMENT - Defined as: "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Thus, ERM deals with risks and opportunities affecting value creation or preservation.	**Five interrelated components of Internal Control as per COSO (CRIME):** • **C**ontrol Activities - Actions …… to manage and reduce risks • **R**isk Assessment - identify and analyse risks faced by an organisation to manage them. • **I**nformation and Communication - Elements to identify, capture and exchange information …..to allow personnel to discharge their responsibilities • **M**onitoring - Elements that ensure Internal Controls operate reliably over time • Control **E**nvironment - The control consciousness of the organization	**Responsibility for Implementing Internal Controls:** Per SOX, the CEO & CFOs personally and criminally liable for the quality and effectiveness of their organization's internal controls over financial reporting. Clause 49 of the listing agreements issued by SEBI in India is on similar lines of SOX regulation and mandates inter alia the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation. Further, it also provides for certification of these aspects by the external auditors.	**COBIT - IT GOVERNANCE MODEL : COBIT 5** • is the business framework for Governance and Management of Enterprise IT • helps enterprises create optimal value from IT by maintaining balance between realising benefits and optimising risk levels & resource use.
COBIT 5 - Principles • **Principle 1:** Meeting Stakeholder Needs – Provides all of required processes and other enablers to support business value creation through the use of IT. Value Creation = Benefits Realisation at Optimisation (Risks + Resources)	• Can be customised to suit diff. obj. of diff. org. through goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific processes and practices.	• **Principle 2:** Covering Enterprise End-to-End - Integrates Governance of Enterprise IT (GEIT) into enterprise governance. It considers all IT related governance and management enablers to be enterprise-wide and end-to-end.	**Principle 3:** Applying a Single Integrated Framework - COBIT 5 aligns with other latest relevant standards and frameworks can be used as the overarching governance & management framework integrator.

Principle 4: Enabling a Holistic Approach - Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components (enablers). Organisations must always consider an interconnected 'set of enablers', since each enabler needs the input of other enablers and Delivers output to the benefit of other enablers	**Principle 5:** Separating Governance from Management - COBIT makes a clear distinction between governance and management. Governance = Evaluate Direct Monitor. Management = Plan Build Run Monitor	**COBIT 5 – Enablers** 1. *Principles, policies and frameworks:* are vehicles to translate desired behaviour into practical guidance. 2. *Processes:* describe an organised set of practices & activities to achieve certain objectives. 3. *Organizational structures:* are the key decision-making entities in an enterprise.	4. *Culture, ethics and behaviour:* are important success factor in gover. & manag. activities. 5. *Information:* is pervasive - includes all information produced and used by enterprise. 6. *Services, infrastructure and applications:* include infrastructure, technology and applications. 7. *People, skills & competencies:* required for successful completion of all activities and for making correct decisions.
COBIT 5 - Process reference model - Defines and describes in detail a number of governance and management processes. It represents all of the processes normally found in an enterprise relating to IT activities. Each enterprise must define its own process set, taking into account its specific situation. It provides a framework for measuring and monitoring IT performance, providing IT assurance, communicating with service providers, and integrating best management practices.	**Using COBIT 5 Best Practices for GRC:** • Defining clearly what GRC requirements are applicable; • Identifying the regulatory and compliance landscape • Reviewing the current GRC status; • Determining the most optimal approach; • Setting out key parameters on which success will be measured;	• Using a process oriented approach; • Adapting global best practices as applicable; and • Using uniform and structured approach which is auditable. **Using COBIT 5 best practices frameworks ensures that all aspects of GRC are implemented.**	**Measuring successful implementation of GRC:** specific success can be measured by using following goals and metrics: **Redundant Controls:** Reduction **Control Failures:** Reduction **Expenditure relating to legal, regulatory and review areas:** Reduction **Overall time required for audit:** Reduction

Process Improvement: Through streamlining of processes and reduction in time through automation of control and compliance measures Timely reporting of regular compliance issues and remediation measures: Improvement Dashboard of overall compliance status and key issues to senior management on a real-time basis as required.	**RISK MANAGEMENT IN COBIT 5** **"EDM03:** Ensure risk optimization": Focuses on stakeholder risk-related objectives. **Ensures:** • Enterprise's risk appetite & tolerance are understood, articulated & communicated, and • That risk to enterprise value related to the use of IT is identified and managed. • Provides guidance on how to ensure that: • IT-related enterprise risk does not exceed risk appetite and risk tolerance,	• the impact of IT risk to enterprise value is identified and managed and • potential for compliance failure is minimised. • Align, Plan & Organise - "APO 12 – Manage Risk" • Primary purpose: • To integrate management of IT-related enterprise risk with overall ERM, and • Manage cost & benefits of managing IT related enterprise risks.	• **Requires:** Continuously identifying, assessing and reducing IT-related risk within the tolerance level set by executive management. Key Governance practices of Risk management Evaluate Risk (Management): examine and make judgement… that risks to enterprise value related to the use of IT are identified and managed. Direct Risk Management: Direct the establishment of risk management practices **Monitor Risk Management:** Monitor the key goals and metrics of the risk management processes
Key Management Practices of Risk Management: • **Collect Data:** Identify and collect relevant data to enable IT related risk identification, analysis and reporting. • **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors. • **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes	• **Articulate Risk:** Provide information on current state of IT- related exposures & opportunities to all required stakeholders. • **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio. **Respond to Risk:** In timely manner to limit magnitude of loss from IT related events.	**Metrics of Risk Management** • Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment; • Number of significant IT related incidents that were not identified in risk Assessment; • Percentage of enterprise risk assessments including IT related risks; and • Frequency of updating the risk profile based on status of assessment of risks.	**IT COMPLIANCE REVIEW:** In the US, Sarbanes Oxley Act (SOX) has been passed to protect investors by improving the accuracy and reliability of corporate disclosures. In India, Clause 49 of listing agreement (similar to SOX) issued by SEBI mandates similar implementation of ERM and internal controls as appropriate for the enterprise.

It requires the CEO / CFO to accept responsibility for – establishing and maintaining internal controls for financial reporting and – that they have evaluated effectiveness of internal control systems of company pertaining to financial reporting and – they have disclosed to the auditors and the Audit Committee, deficiencies in the design or operation of such internal controls, if any, of which they are aware and – the steps they have taken or propose to take to rectify these deficiencies. There are similar legislations in Australia, Japan and other countries.	Reporting on Internal control requirements are also mandated by the Indian Companies Act, 1956 for all companies and a separate annexure to the audit report has to be provided by auditors as per Companies (Auditor's Report) Order, 2003 (CARO). Further, ITAA, 2008 also mandates responsibilities for protecting information (S. 43A). The Act also identifies various types of cyber-crimes and has imposed specific responsibilities on corporate.	In USA, the PCAOB has come out with detailed guidelines on Compliance by Auditors and Companies under the Act. In India, no such guidance is available for Companies and Auditors other than limited guidance from the ICAI to its members, which focuses primarily on audit requirements.	**MEA03 - Monitor, Evaluate & Assess Compliance with External Requirements:** **Primary purpose:** Is to ensure that the enterprise is compliant with all applicable external requirements. **Designed to evaluate:** that IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. **Requires:** That the enterprise has processes in place to obtain assurance and that these requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.
Key Management Practices of IT Compliance: • Identify External Compliance Requirements • Optimize Response to External Requirements • Confirm External Compliance • Obtain Assurance of External Compliance	Key Metrics for Assessing Compliance Process • Compliance with External Laws and Regulations ▪ Cost of IT non-compliance, including settlements & fines; ▪ Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment;	▪ Number of non-compliance issues relating to contractual agreements with IT service providers; and ▪ Coverage of compliance assessments. • IT Compliance with Internal Policies: These metrics are given as follows: • Number of incidents related to non-compliance to policy;	• Percentage of stakeholders who understand policies; • Percentage of policies supported by effective standards and working practices; and • Frequency of policies review and updates

Sample Areas of GRC for Review by Internal Auditors provided by IIA: • Scope • Governance • Evaluate Enterprise Ethics • Risk Management • Interpretation • Risk Management Process • Evaluate Risk Exposures • Evaluate Fraud and Fraud Risk • Address Adequacy of Risk Management Process	**Evaluating IT Governance Structure and practices** by Internal Auditor outlined by IIA, which can be reviewed as a part of Internal audit: • Leadership • Organizational Structure • Processes • Risks • Controls • Performance Measurement / Monitoring	**Evaluating & Assessing System of Internal Controls in COBIT 5** "**MEA 02 -** Monitor, Evaluate & Assess System of Internal Control" **Primary purpose:** • Plan, organize and maintain standards for internal control assessment and assurance activities. • Continuously monitor & evaluate control environment, including self- assessments and independent assurance reviews & • Review provides assurance to key stakeholders on transparency and adequacy of system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risks.	**Key management practices for assessing and evaluating internal controls** • Monitor Internal Controls • Review Business Process Controls Effectiveness • Perform Control Self-assessments • Identify and Report Control Deficiencies • Ensure that assurance providers are independent and qualified • Plan Assurance Initiatives • Scope assurance initiatives

CHAPTER 2 – INFORMATION SYSTEMS CONCEPTS

SYSTEM: A set of interrelated elements that operate collectively to accomplish some common purpose or goal.

TYPES OF SYSTEM

1. **Elements:**
   - Abstract system
   - Physical system
2. **Interactive Behaviour:**
   - Closed System
   - Relatively Closed System
   - Open System
3. **Degree of Human Intervention :**
   - Manual System
   - Automated System
4. **Working / Output -**
   - Deterministic System
   - Probabilistic System

GENERAL MODEL OF A SYSTEM: A general model of a physical system is input, process and output. A system may have several inputs and outputs. The elements of a system are:

- Input
- Processing
- Output
- Storage
- Feedback

SYSTEM ENVIRONMENT

- **Boundary :** The features that define and delineate a system form its boundary.
- **Subsystem :** A subsystem is a part of a larger system.
- **Interfaces:** The inter connections and interactions between the subsystem are termed interfaces.

Decomposition / Factoring – process by which a system is broken down into parts that are easier to conceive, understand, program, and maintain.

Simplification - process of organizing subsystems so as to reduce the number of interconnections.

Decoupling – Is to identify the separation of sub subsytems (software blocks) that shouldn't depend on each other.

INFORMATION: Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision.

CHARACTERISTICS OF INFORMATION: (Charmy's **CAR** has **MRF T**yres and **V**oice **R**ecorder**)**

- **C**ompleteness
- **C**ost Benefit Analysis
- **A**ccuracy and Quality
- **R**elevance and Purpose
- **M**ode and Format
- **R**edundancy
- **F**requency
- **T**imeliness
- **V**alidity
- **Reli**ability

TYPES OF INFORMATION :

- Internal information
- External information

INFORMATION SYSTEM AND ITS ROLE IN MANAGEMENT: An information system can be considered as an arrangement of a number of elements that provides effective information for decision-making and / or control of some functionalities of an organization. Implications:

- Decision-making
- Competitive edge
- Innovative ideas
- Knowledge
- Formulate a strategy

FACTORS ON WHICH INFORMATION REQUIREMENTS DEPEND:

1. Operational function
2. Type of decision making :
   - Programmed decisions or structured decisions
   - Non-programmed or unstructured decisions
3. Level of management activity :
   - Strategic Level or Top level
   - Tactical Level or middle
   - Supervisory or operational Level

COMPONENTS OF COMPUTER BASED INFORMATION SYSTEM: A Computer-based Information System (CBIS) is an information system in which the computer plays a major role. Such a system consists of the following elements:

- Hardware
- Software
- Data Procedures
- People

OPERATIONS SUPPORT SYSTEMS (OSS)

- Transaction Processing Systems - TPS
- Management Information Systems – MIS
- Enterprise Resource Planning Systems – ERP

TRANSACTION PROCESSING SYSTEM (TPS) : It involves

- Capturing data
- Processing of files / databases
- Generating information
- Handling of queries

TPS COMPONENTS

- Inputs
- Processing
- Storage
- Outputs

FEATURES OF TPS (LABS)

- **L**arge volume of data
- **A**utomation of basic operations
- **B**enefits are easily measurable
- **S**ource of input for other systems

MANAGEMENT INFORMATION SYSTEM (MIS) : An integrated user-machine system designed for providing information to support operational control management control and decision making functions in an organization.

CHARACTERISTICS OF AN EFFECTIVE MIS: (M2IC2S is **H**istory**)**

- **M**anagement Oriented
- **M**anagement Directed
- **I**ntegrated
- **C**ommon Database
- **C**omputerised
- **S**ub system concept
- **H**eavy Planning Element

MISCONCEPTIONS OR MYTHS ABOUT MIS:

- The study of management information system is about the use of computers.
- More data in reports means more information., for managers
- Accuracy in reporting is of vital importance

PRE-REQUISITES OF AN MIS: (D - CESS)

- **D**atabase
- **C**ontrol and Maintenance of MIS
- **E**valuation of MIS
- **S**ystem and Management staff should be qualified
- **S**upport of Top Management

CONSTRAINS IN OPERATING A MIS: (Q2ES3)

- **Q**ualified staff not available
- **Q**uantifying the benefits of MIS is difficult
- **E**xpert's turnover is high
- **S**election of Sub system of MIS
- **S**tandardised approach not possible
- **S**taff's Cooperation not available

EFFECTS OF USING COMPUTER IN MIS: (I2S2C2A)

- **I**ncreases the effectiveness of Information Systems
- **I**ntegrates the working of different information subsystem
- **S**peed of processing and retrieval of data increases
- **S**cope of use of information system has expanded
- **C**omplexity of system design and operation increased
- **C**omprehensive information
- **A**nalysis widens

LIMITATIONS OF MIS:

- Less useful for unstructured data
- Internal information is taken into consideration
- Management keeps changing so does their goals
- inputs and processing quality determines the quality of outputs
- IPS's limitations still exists in MIS
- Ad-hoc reporting is not possible
- The Attitudes and moral are ignored in MIS
- Integration is lacking
- Hoarding of information reduces the effectiveness
- Not a substitute for effective management

ENTERPRISE RESOURCE PLANNING (ERP) SYSTEMS:

- ERP system is a fully integrated business management system
- It organizes and integrates - operation processes and information flows, to make optimum use of resources
- ERP aims at one database, one application, and one user interface

OBJECTIVES :

- Provide support for adopting best business practices
- Implement these practices with a view towards enhancing productivity
- Empower the customers and suppliers to modify the implemented business processes to suit their needs

AN ERP SYSTEM INTEGRATES VARIOUS BUSINESS PROCESSES :

- Business System
- Production
- Maintenance
- Quality Control
- Marketing
- Finance
- Personnel
- Consolidation of Business Operations

MYTHS OF ERP SYSTEM :

- ERP is a computer system.
- ERP is relevant for manufacturing organizations only.

BENEFITS OF ERP:

- Better use of Organizational Resources
- Lower Operating Costs
- Proactive Decision Making
- Enhanced customer Satisfaction
- Flexibility in Business Operations

LIMITATIONS OF ERP :

- An ERP system provides current status only
- The methods used in the ERP applications are not integrated with other organizational or divisional systems.

Data mining (DM) -

Is applied in database analysis and decision support i.e. market analysis and management by finding patterns that are helpful in target marketing, customer relation management, market basket analysis, cross selling, market segmentation, risk analysis, customer retention, etc.,

Business Intelligence (BI) –

Refers to applications and technologies that are used to collect, provide access and analyse data and information about companies operations.

MANAGEMENT SUPPORT SYSTEMS (MSS): focus on the managerial uses of information resources and provide information to managers for planning and decision making. There are three types of MSS, namely:

- Decision Support Systems (DSS)
- Executive Information (Support) System (EIS)
- Expert Systems.

DECISION SUPPORT SYSTEMS (DSS) : is a system that provides tools to managers to assist them in solving semi structured and unstructured problems in their own, somewhat personalized, way.

CHARACTERISTICS OF DSS: (SEA)

- Support Semi-structured / Unstructured decision making
- Ease of Learning and Use
- Ability to adapt to changing need

COMPONENTS OF A DSS :

- The User:
  - Manager, does not have IT background
  - Has through understanding of the factors to be considered in finding solution
- Databases: Implementation at 3 levels
  - Physical level
  - Logical Level
  - External level
- A planning language
- General Purpose - Excel
- Special Purpose – SAS, SPSS
- Model Base – Brain of DSS

EXECUTIVE INFORMATION SYSTEMS (EIS): Tool designed to meet special needs of top-level managers.

Provides direct on-line access to relevant information in a useful and navigable format.

EXECUTIVE ROLES AND DECISION MAKING :

- Strategic Planning – Long range Direction
- Tactical Planning – General Tactics
- Fire Fighting – Resolving major problems
- Control – Feedback

PRINCIPLES TO BE FOLLOWED WHILE DESIGNING AN EIS:

EIS must be :

- Easy to understand and collect
- Based on a balanced view of the organisation's objectives
- Reflecting everyone's contribution in a fair and consistent way
- Encouraging for the management and staff
- Available to everyone in the organization.
- Evolving to meet the changing needs of the organization.

EIS SERVES THE FOLLOWING PURPOSE : (STD Bill)

- **S**upport managerial learning
- **T**imely access to information
- **D**irects the attention of the management
- **B**alanced view

CHARACTERISTICS OF THE TYPES OF INFORMATION USED IN EXECUTIVE DECISION-MAKING: (SUFI Lyrics**)** • **S**tructure is lacking • High degree of **U**ncertainty • **F**uture orientation • **I**nformal source • **L**ow Level of detail	**EXPERT SYSTEMS** Expert Systems are software systems that imitate the reasoning process of human experts and provide decision makers with the type of advice they would normally receive from such expert systems	**NEED FOR EXPERT SYSTEMS** • Expert labour is expensive and scarce. • No matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.
BENEFITS OF EXPERT SYSTEMS • preserve knowledge • put information into an active-form • assist novices in thinking the way experienced professional do. • not subject to such human • fallings as fatigue, being too busy, or being emotional • can be used as strategic tool is areas of marketing products, cutting costs and improving products.	Properties potential applications should possess to qualify for development of expert system: (Dolly's Sister Can Eat Apples) • **D**omain • **S**tructure • **C**omplexity • **E**xpertise • **A**vailability	**COMPONENTS OF EXPERT SYSTEMS** • Knowledge Base (KB) • Inference Engine - forward-chaining mechanism - backward chaining mechanism • Knowledge Acquisition Subsystem (KAS) • User Interface
OFFICE AUTOMATION SYSTEMS (OAS): (Files are Created, Captured, Calculated and Recorded & Distributed): is the application of computers to handle the office activities. • Filling, Search, Retrieval and Follow up • Document Creation • Document Capture • Calculations • Recording Utilization of Resources • Receipts and Distribution	**BENEFITS OF OFFICE AUTOMATION SYSTEMS** • Improve communication • Reduce the cycle time between preparation and receipt of messages • Reduce the costs of office communication • Ensure accuracy of communication flows.	**CATEGORIES OF COMPUTER BASED OFFICE AUTOMATION SYSTEMS:** • Text Processing Systems • Electronic Document Management Systems • Electronic Message Communication Systems • Teleconferencing and Video-conferencing Systems

CHAPTER 3: PROTECTION OF INFORMATION ASSETS

WHAT IS INFORMATION SYSTEM SECURITY: The protection of the interests of those relying on information. Security Objective (**CIA**) • **C**onfidentiality - Data and information are disclosed only to those who have a right to know it • **I**ntegrity - Data and information are protected against unauthorised modification • **A**vailability - Information systems are available and usable when required	**IMPORTANCE OF INFORMATION SYSTEM SECURITY:** Significance of information is widely accepted. Organisations depend on timely, accurate, complete, valid, consistent, relevant and reliable Inf. Many direct and indirect risks which lead to a gap between the need to protect and degree of protection applied. It may result in both financial / intangible losses. Threats may arise from intentional or unintentional acts. Threats may be from internal or external sources. Adequate measures help to ensure smooth functioning	**WHAT INFORMATION IS SENSITIVE** • Strategic Plans • Business Operations • Finances
INFORMATION SECURITY POLICY: Is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organisation	**INFORMATION SECURITY POLICY, STANDARDS, BEST PRACTICES & GUIDELINES, PROCEDURES** **IS POLICY:** Broad general management statement. **IS Standard:** Specify the (compulsory & uniform) technologies and methodologies to be used to secure systems. **IS Best practice:** Guidelines help in smooth implementation of information security policy. **IS Procedure:** Detailed steps to be followed to accomplish particular security related tasks.	**ISSUES TO ADDRESS:** • A definition of information security • Reasons why information security is important to the organisation, and its goals and principles • A brief explanation of the security policies, principles, standards and compliance requirements • Definition of all relevant information, security responsibilities • Reference to supporting documentation

TYPES OF INFORMATION SECURITY POLICIES AND THEIR HIERARCHY: (**U A**nd **I C**an **O**bviously **N**ail **I**t) • **U**ser Security Policy • **A**cceptable Usage Policy • **I**nformation Security Policy • **C**onditions of Connection • **O**rganisational Information Security Policy • **N**etwork & System Security Policy • **I**nformation Classification Policy	**COMPONENTS OF SECURITY POLICY :** • Purpose and Scope of the Document and the intended audience • The Security Infrastructure • Security policy document maintenance and compliance requirements • Incident response mechanism and incident reporting • Security organization Structure • Inventory and Classification of assets • Description of technologies and computing structure • Physical and Environmental Security • Identity Management and access control • IT Operations management • IT Communications • System Development and Maintenance Controls • Business Continuity Planning • Legal Compliances • Monitoring and Auditing Requirements Underlying Technical Policy	**CONTROL:** 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.
IMPACT OF TECHNOLOGY ON INTERNAL CONTROLS: **Major components of Internal control and how they are affected:** • Segregation of duties • Delegation of Authority and responsibility • Documents and records • Personnel – Recruitment and training • Access to assets and records • Management supervision and review • Comparison – Records & physical • Authorisation procedures	**Five interrelated components of Internal Control as per COSO (CRIME):** • **C**ontrol Activities • **R**isk Assessment • **I**nformation and Communication • **M**onitoring • **C**ontrol Environment	**OBJECTIVE OF CONTROLS:** The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. Some categories of exposures are: • Errors or omissions • Improper authorizations and improper accountability • Inefficient activity • Some of the critical control considerations in a computerized environment are • Lack of management understanding of IS risks

• Absence or inadequate IS control framework. • Absence of or weak general controls and IS controls. • Lack of awareness and knowledge of IS risks • Complexity of implementation of controls • The control objectives serve two main purposes : • Outline the policies of the organization as laid down by the management. • A benchmark for evaluating whether control objectives are net.	**CATEGORISATION OF CONTROLS -** Based on the objective with which controls are designed or implemented: • Preventive Controls • Detective Control • Corrective Controls • Compensatory Controls **Based on the nature of such controls with regard to the nature of IS resources to which they are applied :** (Mature Partner Ensures Overall Stable Life) • IS Management Controls • Physical Access Controls • Environmental controls • IS Operational Controls • SDLC Controls • Logical Access Controls **Category of controls is based on their functional nature/ Component of Internal Control:**(I Am Old) • Internal Accounting controls • Administrative controls • Operational controls	**CONTROL TECHNIQUES:** • Organizational Controls • Management Controls • Financial Control Techniques • Data Processing Environment Controls • Physical Access Controls • Logical Access Controls • SDLC (System Development Life Cycle) Controls • Business Continuity (BCP) Controls • Application Control Techniques
ORGANIZATIONAL CONTROLS • Reporting responsibility and authority of each function, • Definition of responsibilities and objectives of each functions, • Policies and procedures, • Job descriptions, • Segregation of duties.	**MANAGEMENT CONTROLS** • Responsibility • An official IT structure • An IT steering committee	**FINANCIAL CONTROL TECHNIQUES :** • Authorization • Budgets • Cancellation of documents • Documentation • Dual control • Input / output verification • Supervisory review

ACCESS CONTROL MECHANISMS

Three steps – (IAA)

- **I**dentification - the users have to identify themselves, thereby indicating their intent to request the usage of system resources.
- **A**uthentication - Users must authenticate themselves & mechanism must authenticate itself.
- **A**uthorisation - Users request for specific resources, their need for those resources & their areas of usage of these resources.
  - Ticket oriented approach
  - List-oriented approach

LOGICAL ACCESS CONTROLS

- Logical access controls restrict users to authorized transactions and functions.
- There are logical controls over network access.
- There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

LOGICAL ACCESS PATHS : (DOOT)

- **D**ial-up Ports
- **O**nline Terminals
- **O**perator Console
- **T**elecommunication Network

LOGICAL ACCESS ISSUES AND EXPOSURES :

- Access control software
- Application software
- Data
- Data dictionary
- Password library
- Telecommunication lines

ISSUES AND REVELATIONS RELATED TO LOGICAL ACCESS:

1. **Technical Exposures:** (**W**orms **D**estroyed **R**ace **H**orse by **T**hrowing **B**ombs)
   - **W**orms
   - **D**ata Diddling
   - **R**ounding Down
   - **T**rojan Horse
   - Salami **T**echniques
   - **B**ombs: Time Bomb or Logic Bomb
2. **Asynchronous Attacks:** (**P**igs **L**ove **T**o **D**ance)
   - **P**iggybacking:
   - Data **L**eakage
   - Wire **T**apping
   - **D**enial of Service
3. **Computer Crime Exposures:** (**C**rime **S**eems **L**ucrative **B**ut **D**oesnot **S**ustain **F**orever)
   - Loss of **C**redibility / **C**ompetitive Edge
   - **S**abotage
   - **L**egal Repercussions
   - Industrial Espionage / **B**lackmail
   - **D**isclosure of Confidential, Sensitive or Embarrassing Information
   - **S**poofing
   - **F**inancial Loss

USER CONTROLS - (BIPOD) • **B**oundary Controls • **I**nput Controls • **P**rocessing Controls • **O**utput Controls • **D**atabase Controls	**USER CONTROLS: ERROR IDENTIFICATION, CORRECTION AND RECOVERY CONTROLS: (PIN and Passwords are C**oded **on ICards)** Boundary control technics are : • Personal Identification Numbers (PIN) • Passwords • Cryptography • Identification Cards	**Input Controls: Factors affecting coding errors are as follows:** **(S**unny **L**ehman **M**arried **C**hartered **A**ccountant**)** • **S**equence of characters • **L**ength of the code • **M**ixing uppercase/lowercase fonts • **C**hoice of characters • **A**lphabetic numeric mix
Processing Controls: (Runners **E**at **E**ggs **F**or **R**unning**)** • **R**un-to-run totals • **E**dit checks • **E**xception reports • **F**ield initialization • **R**easonableness verification	**Output Controls: (Spools** & **Logs R**equire **Retaining, Storing, Reporting** and **Printing)** • Spooling/Queuing • Logging of output program executions • Recovery Controls • Retention Controls • Storage of sensitive, critical forms • Report distribution and collection controls • Printing Controls	**Database Controls:** The update controls are: • Sequence Check Transaction and if Master Files • Ensure All Records on Files are processed • Process multiple transactions for a single record in the correct order • Maintain a suspense account **Database Controls:** The Report controls are: • Standing Data • Print Run-to-Run control Totals • Print Suspense Account Entries • Recovery Controls

DATA INTEGRITY: Primary objective is to prevent, detect, and correct errors in transactions as they flow through the various stages of a specific date processing program. (**OOPS I**nformation **T**echnology) • **O**n-line Data Entry controls • **O**utput controls • Data **P**rocessing and storage controls • **S**ource data control • **I**nput validation routines • Data **T**ransmission controls	**DATA INTEGRITY POLICIES** • Virus-Signature Updating • Software Testing • Division of Environments • Version Zero Software • Offsite Backup Storage • Quarter-End and Year-End • Disaster Recovery	**LOGICAL ACCESS CONTROL ACROSS THE SYSTEM** • User access management • User registration • Privilege management. • User password management • Review of user access rights • User responsibilities - Password use - Unattended user equipment • Network access control - Policy on use of network services - Enforced path - Segregation of networks - Network connection and routing control Security of network services
• **Operating system access control** - Automated terminal identification - Terminal log-on procedures - User identification and authentication - Password management system - Use of system utilities - Duress alarm to safeguard users - Terminal time out • Limitation of connection time	• **Application and monitoring system access control** - Information access restriction - Sensitive system isolation - Event logging - Monitor system use • Clock synchronization • **Mobile computing** - Mobile computing	**PHYSICAL ACCESS CONTROLS: PHYSICAL ACCESS ISSUES AND EXPOSURES -** • Abuse of data processing resources. • Blackmail • Embezzlement • Damage, vandalism or theft to equipment's or documents. • Modification of semester equipment and Information. • Public disclosure of sensitive Information. • Unauthenticated entry

PHYSICAL ACCESS CONTROLS

1. Locks on Doors
   - Cipher locks
   - Bolting Door Locks
   - Electronic Door Locks
   - Biometric Door Locks
2. Physical identification medium
   - Personal Identification numbers (PIN)
   - Plastic Cards
   - Cryptographic Control
   - Identification Badges
3. Logging on utilities
   - Manual Logging
   - Electronic Logging
4. Other means of controlling Physical Access like: Video Cameras, Security Guards, Controlled Visitor Access, etc.

CONTROLS FOR ENVIRONMENTAL EXPOSURES/AUDIT AND EVALUATION TECHNIQL ES FOR ENVIRONMENTAL CONTROLS:

- Hand-Held Fire Extinguishers
- Manual Fire Alarms
- Fire Suppression Systems:
  - Dry-Pipe sprinkling Systems
  - Water based systems
  - Halon systems
- Regular Inspection by Fare Department
- Water Detectors
- Smoke Detectors
- Strategically Locating the Computer Room
- Fireproof Walls, Floors and Ceilings surrounding the Computer Room
- Electrical Surge Protectors
- Uninterruptible Power Supply (UPS)/Generator
- Power Leads from Two Substations
- Emergency Power-Off Switch
- Wiring Placed In electrical panels & conduit
- Prohibitions against eating, drinking and Smoking within the information Processing Facility
- Documented and Tested Emergency Evacuation Plans

ROLE OF IS AUDITOR IN PHYSICAL ACCESS CONTROLS :

- Risk assessment
- Controls assessment
- Planning for review of physical access controls
- Testing of controls

ENVIRONMENTAL CONTROLS: ENVIRONMENTAL ISSUES AND EXPOSURES - • Fire • Natural disasters • Power spike • Air conditioning failure • Electrical shock • Equipment failure ; • Water damage / flooding • Bomb threat / attack	**CYBER FRAUDS:** **mean** frauds committed by use of technology. **Two types:** • Pure Cyber Frauds: Frauds, which exists only in cyber world. They are borne out of use of technology. For example: Website hacking. • Cyber Enabled Frauds: Frauds, which can be committed in physical world also but with use of technology; the size, scale and location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.	**Cyber Attacks** • Phishing: • Network Scanning: • Virus/Malicious Code: • Spam: • Website Compromise / Malware Propagation: • Cracking: • Eavesdropping: • E-mail Forgery: • E-mail Threats: • Scavenging
Impact of Cyber Frauds on Enterprises • Financial Loss: • Legal Repercussions: • Loss of credibility or Competitive Edge: • Disclosure of Confidential, Sensitive or Embarrassing Information: • Sabotage:	**Techniques to Commit Cyber Frauds** • Hacking: • Cracking: • Data Diddling: • Data Leakage: • Denial of Service (DoS) Attack: • Internet Terrorism: • Logic / Time Bombs: • Masquerading or Impersonation:	• Password Cracking: • Piggybacking: • Round Down: • Scavenging or Dumpster Diving: • Social Engineering Techniques: • Super Zapping: • Trap Door:

CHAPTER 4: BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY PLANNING

Basic Terms

(1) Business Contingency:

Is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions.

(2) Business Continuity:

Means maintaining the uninterrupted availability of all key business resources required to support essential business activities.

Thus, Business continuity covers the following areas:

- Crisis management
- Disaster recovery planning
- Business resumption planning

(3) Business Continuity Planning (BCP):

Refers to the ability of enterprises to recover from a disaster and continue operations with least impact. (For details refer relevant para below)

(4) BCP Process:

Is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations 3.

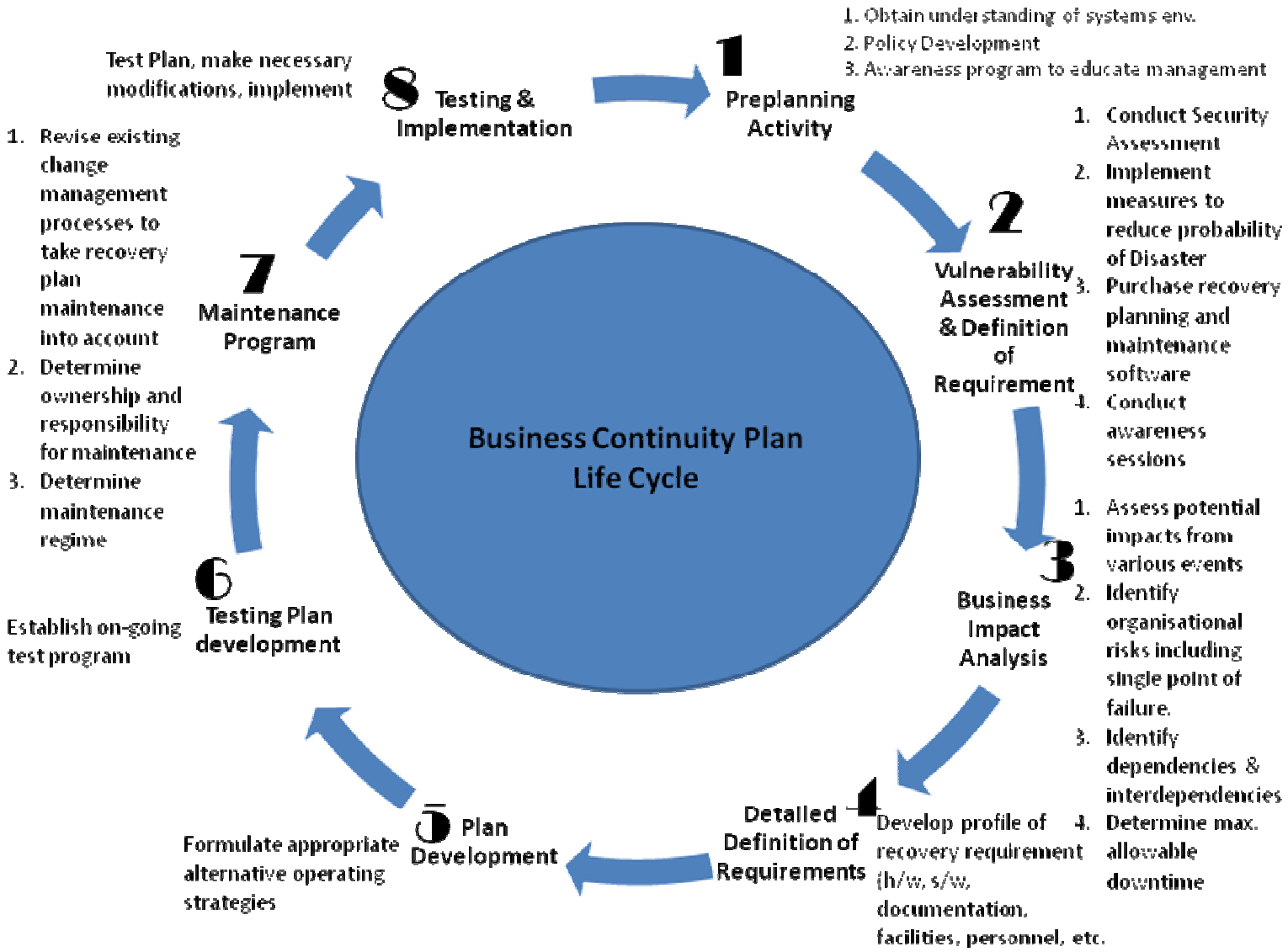
(5) BCM team:

It's mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions.

(6) BCP Manual:

Is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations.

Phases of Business Continuity Planning



BUSINESS CONTINUITY PLANNING is the creation and validation of a practical logistical plan for how an organization will recover and

restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption.

Business continuity plan covers:

- Business resumption planning
- Disaster recovery planning
- Crisis management

OBJECTIVES AND GOALS OF BUSINESS CONTINUITY PLANNING

The Objectives: - Primary objective is to enable an organisation to survive a disaster and to re-establish normal business operations.

- Provide for safety of people on the premises at the time of disaster
- Continue critical business operations,
- Minimise the duration of a serious / disruption to operations and resources
- Minimise immediate damage and losses
- Establish management succession and emergency powers
- Facilitate effective coordination of recovery tasks
- Reduce complexity of recovery effort Identify critical lines of business and supporting functions The goals of Business Continuity Plan:
- Identify weaknesses and implement a disaster prevention program
- Minimise the duration of a serious disruption to business operations
- Facilitate effective co-ordination of recovery tasks
- Reduce the complexity of the recovery effort

DEVELOPING BUSINESS CONTINUITY PLAN:

- Providing an understanding of the efforts required to develop and maintain a recovery plan to the management
- Obtaining Commitment from management
- Defining recovery requirements from the perspective of business functions
- Document impact of an extended loss to operations and key business functions
- Focusing appropriately on disaster prevention and Impact minimization.
- Selecting business continuity teams
- Developing a business continuity plan.
- Defining integration into on-going business planning and system development processes

PHASES OF BUSINESS CONTINUITY PLANNING: (Pakistan **V**s **B**angladesh **D**elayed **P**laying **T**heir **M**atch in **I**ndia**)** **I.** **P**re-planning Activity II. **V**ulnerability Assessment III. **B**usiness Impact Analysis IV. **D**etailed Definition of Requirement V. **P**lan Development VI. **T**esting Plan Development VII. **M**aintenance Program **VIII.** Testing & **I**mplementation **See chart above** **TYPES OF PLANS (COMPONENTS OF A DISASTER RECOVERY PLAN):** • Emergency Plan • Back-up Plan • Recovery Plan • Test Plan	**DISASTER RECOVERY PROCEPURAL PLAN:** • The conditions for activating the plan • Emergency procedures • Fallback procedures • Resumption procedures • Maintenance schedule • Awareness and education activities • The responsibilities of individuals • Contingency plan testing and recovery procedure. • The purpose and scope of the plan. • Contingency plan testing and recovery procedure. • List of phone numbers of employees • Emergency phone list for fire, police, back-up location, etc. • Medical procedure to be followed • Insurance papers and claim forms • Names of employees trained for emergency situation, first aid and life saving techniques.	**SOFTWARE AND DATA BACK-UP TECHNIQUES - TYPES OF BACK¬UPS: (I M**anaged to **D**raw a **F**lower**)** • **I**ncremental Backup • **M**irror back-up • **D**ifferential Backup • **F**ull Backup
ALTERNATE PROCESSING FACILITY ARRANGEMENTS: • Cold site • Hot site • Warm site • Reciprocal agreement	**BUSINESS CONTINUITY MANAGEMENT (BCM):** Is business-owned, business-driven process that establishes a fit-for-purpose strategic and operational framework that: • Proactively improves enterprise's resilience against disruption.	• rehearsed method of restoring enterprise's ability to supply its key products & services to an agreed level within an agreed time after a disruption; and • Delivers a proven capability to manage a business disruption and protect the enterprise's reputation and brand.

Scope of BCM:

- Is defined by top management by identifying the key products and services that support the enterprise's objectives, obligations and statutory duties in line with the threat scenario and the business impact analysis

BCM Policy:

Defines the processes of setting up activities for establishing a business continuity capability and the on-going management and maintenance of the business continuity capability.

The objective of this policy is to provide a structure through which:

(1) Critical services and activities undertaken by the enterprise operation for the customer will be identified.

(2) Plans will be developed to ensure continuity of key service delivery

(3) Manage Invocation of incident management and business continuity plans.

(4) Subject Incident Management Plans & Business Continuity Plans to on-going testing, revision and updation as required.

(5) Assign Planning and management responsibility to a member of the relevant senior management team.

Advantages of BCM:

The advantages of BCM are that the enterprise:

- is able to proactively assess the threat scenario and potential risks;
- has planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and
- is able to demonstrate a response through a process of regular testing and trainings.

Components of BCM Process

BCM - Management Process

Enables the business continuity, capacity and capability to be established and maintained in accordance with the requirements of the enterprise.

BCM – Information Collection Process

Is the assessment process that does the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them.

BCM – Strategy Process

Requires an appropriate response to be selected, so that the enterprise continues to provide products and services.

BCM – Development and Implementation Process

Develops of business continuity, business recovery and restoration plans and structure of incident management / crisis management team for effective response and recovery.

BCM Testing and Maintenance Process

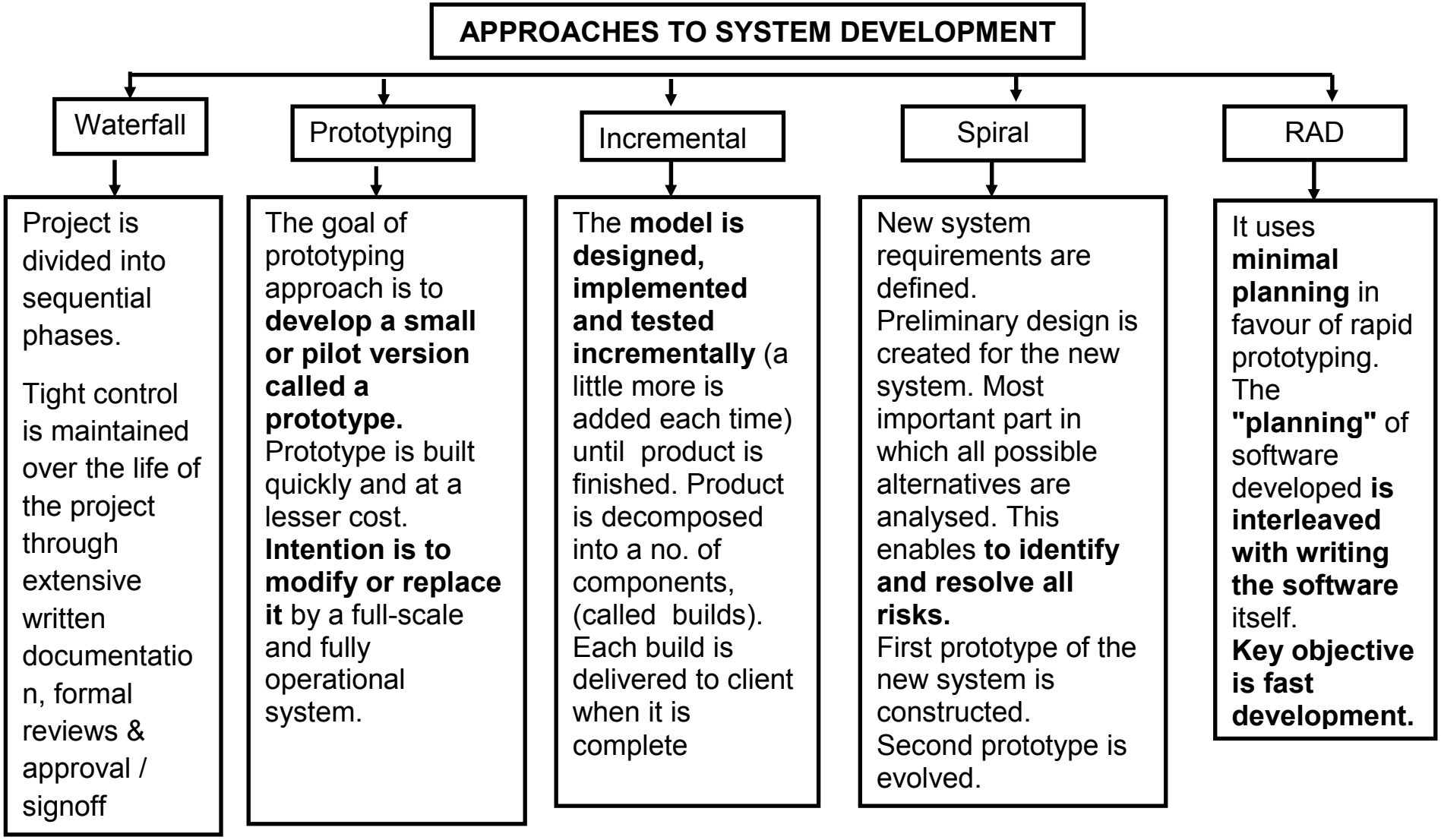
Proves the extent to which enterprise's strategies and plans are complete, current and accurate; and Identifies opportunities for improvement.

BCM Training Process

Enables BCM to become part of the enterprise's core values and provide confidence to all stakeholders in the ability of the enterprise's ability to cope with minimum disruptions and loss of service.

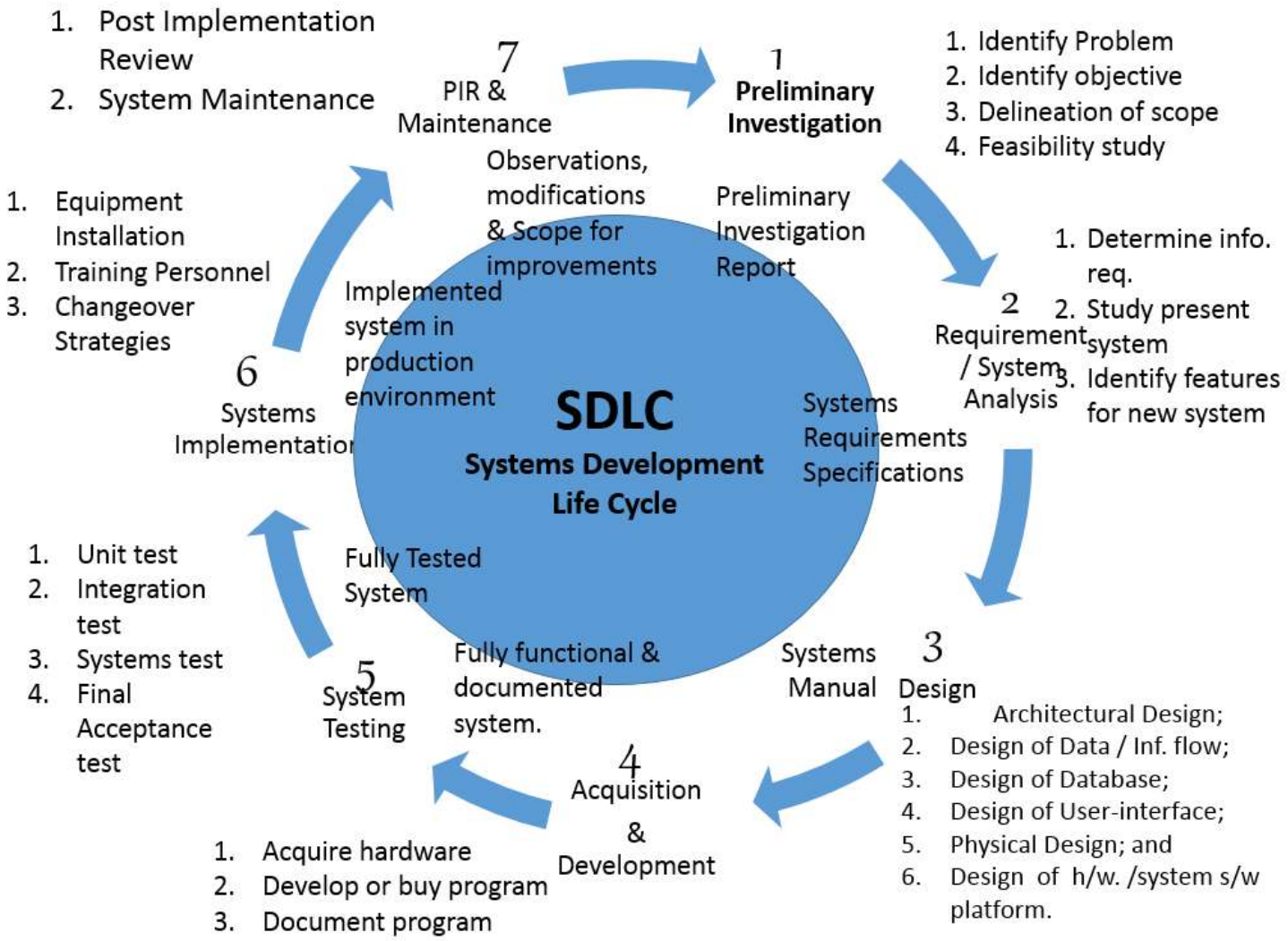
CHAPTER 5: SYSTEMS DEVELOPMENT LIFE CYCLE METHODOLOGY

FLOW CHART: 1



FLOW CHART: 2

PHASES OF SDLC



SYSTEMS DEVELOPMENT PROCESS: Systems development refers to the process of examining a business situation with the intent of improving it through better procedures and methods.

- System Analysis
- System Design

REASONS FOR FAILURE :

- Lack of senior management support for and involvement in information systems development
- Shifting user needs
- Development of strategic systems
- New technologies
- Lack of standard project management and systems development methodologies
- Overworked or under-trained development staff
- Resistance to change
- Lack of user participation
- Inadequate testing and user training

CHARACTERISTICS OF SYSTEM DEVELOPMENT METHODOLOGY:

- The project is divided into a number of identifiable processes
- Deliverables must be produced
- Users, managers, and auditors are required to participate in the project to provide sign-offs.
- The system must be tested thoroughly
- A training plan is developed
- Formal program change controls are established
- A post-implementation review of all developed systems must be performed.

APPROACHES TO SYSTEM DEVELOPMENT

- **Waterfall :** Linear framework type
- **Prototyping:** Iterative framework type
- **Incremental:** Combination of linear and iterative framework type
- **Spiral:** Combination linear and iterative framework type
- **Rapid Application Development : (RAD) :** Iterative Framework Type
- Agile Methodologies

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC): framework provides system designers and developers to follow a sequence of activities. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one.

THE PHASES INVOLVED IN THE SDLC :

1. Preliminary Investigation
2. Systems / Requirements Analysis
3. Systems Design
4. Systems Acquisition & Development
5. Systems Testing
6. Systems Implementation
7. Post Implementation Review and Maintenance

PHASE - I PRELIMINARY INVESTIGATION - OBJECTIVES **Objective :** To determine and analyze the strategic benefits in implementing the system through evaluation and quantification of - productivity gains; future cost avoidance; cost savings and Intangible benefits like improvement in morale of employees. **Document / Deliverable:** A preliminary Investigation report / feasibility study for management.	**IDENTIFICATION OF PROBLEM** • Clarify and understand the project request • Determine the size of the project • Determine the technical and operational feasibility of alternative approaches • Assess costs and benefits of alternative approaches • Report findings to the management with recommendation outlining the acceptance or rejection of the proposal.	**DELINEATION OF SCOPE** • Functionality requirements • Data to be processed • Control requirements • Performance requirements • Constraints • Interfaces • Reliability requirements Methods with the help of which scope of the project can be analyzed are as follows : • Reviewing Internal documents • Conducting Interviews
FEASIBILITY STUDY: (FOSTERL) • **F**inancial • **O**perational • **S**chedule / Time • **T**echnical • **E**conomical • **R**esources (Human) • **L**egal	**ESTIMATING COST & BENEFIT COSTS:** • Development • Operational • Intangible **BENEFITS:** • Tangible • Intangible	**PHASE - II : SYSTEMS REQUIREMENTS ANALYSIS FACT FINDING TECHNIQUES:** (**D**octor **I**nterviews and **Q**uestions while **O**bservation) • **D**ocuments • **I**nterviews • **Q**uestionnaires • **O**bservations
ANALYSIS OF PRESENT SYSTEM • Review Historical Aspects • Analyze inputs • Review Data Files Maintained • Review Methods, Procedures & data **Communications** • Analyze Output • Review Internal Controls • Model Existing Physical & Logical System • Undertake Overall Analysis	**SYSTEMS ANALYSIS OF PROPOSED SYSTEMS:** After each functional area of the present information system has been carefully analysed, the proposed system specifications must be clearly defined.	**SYSTEM DEVELOPMENT TOOLS:** 1. System Components & Flows • System Flow Chart (SFC) • Data Flow Diagram (DFD) • System Components Matrix 2. User Interface • Layout Forms and Screens • Dialogue flow diagrams 3. Data Attributes & Relationship • Data Dictionary • ERD • File Layout Forms • Grid Charts 4. Detailed System Process • Decision Trees • Structure Charts

STRUCTURED ENGLISH :

Program Design Language (PDL) or Pseudo Code, is the use of the English language with the syntax of structured programming. Thus, Structured English alms at getting the benefits of both the programming logic and natural language. Program logic that helps to attain precision and natural language that helps in getting the convenience of spoken languages.

FLOWCHARTS :

Can be used by to represent the input, Output and processes of a business in a pictorial form. It is a common type of chart that represents an algorithm or process showing the steps as boxes of various kinds and their order by connecting these with arrows. Flow charts are used in analyzing, designing, documenting or managing a process of program.

TYPES OF FLOW CHARTS

- Document flowchart
- Data flowchart
- System flowchart
- Program flowchart

BENEFITS OF FLOWCHART:

- Communication
- Effective analysis
- Proper documentation
- Efficient Coding
- Proper Debugging
- Efficient Program Maintenance

LIMITATIONS OF USING FLOWCHARTS :

- Complex logic
- Alterations and Modifications.
- Reproduction
- The essentials of what is done can easily be lost in technical details of how it is done.

DECISION TREE: Or a tree diagram is a support tool that uses a tree-like-graph or model of decisions and their possible consequences, including, chance event outcomes, resource costs, and utility.

DECISION TABLE : is a table which may accompany flowchart, defining the possible contingencies that may be considered within the program and the appropriate course of action for each contingency Condition Stub - which comprehensively lists the comparisons or conditions;

- Condition Stub
- Action Stub
- Condition entries
- Action entries

DATA DICTIONARY: It is a computer file that contains descriptive information about the data items (fields) in the files of a business information system. In other words, it is a computer file about data (items).

Uses :

- Aids in documentation - To Programmers & analysts
- File Security
- For Accountant - Planning flow of transaction data
- For Auditors - Establish audit trail
- Aids in investigation / documenting internal control procedures

Data Dictionary Contains:

- Data item's length, type & range
- Identify of source document used to create data item
- Names of computer file storing data item
- Names of computer programs that modify data Item
- Identity of individual permitted to access
- Identity of Individual not permitted to access

LAYOUT FORM AND SCREEN GENERATOR, MENU GENERATOR, REPORT GENERATOR, CODE GENERATOR

- Layout form and Screen Generator
- Menu Generator
- Report Generator
- Code Generator

SYSTEM SPECIFICATION

At the end of the analysis phase, the systems analyst prepares a document called "Systems Requirement Specifications (SRS)", it contains:

- Introduction
- Information Description
- Functional Description
- Behavioural Description
- Validation Criteria
- Appendix
- SRS Review

ROLES INVOLVED IN SDLC

- Steering Committee
- Project Manager
- Project Leader
- Systems Analyst / Business Analyst
- Module Leader/Team Leader
- Programmer / Coder / Developer
- Database Administrator (DBA)
- Quality Assurance
- Tester
- Domain Specialist
- IS Auditor

PHASE - III: SYSTEM DESIGN

System design involves first logical design and then physical construction of a system. Design specifications Instruct programmers about what the system should do. The programmers, in turn, write the programs that accept input from users, process data, produce the reports, and store data in the files.

THE DESIGN PHASE INVOLVES :

- Architectural Design
- Design of the Data / Information Flow
- Design of the Database
- Design of the User-interface
- Physical Design
- Design of hardware / system software platform

DESIGN OF DATABASE

- Conceptual Modeling
- Data Modeling
- Storage Structure Design
- Physical Layout Design

DESIGN OF USER-INTERFACE

Output Objectives :

- Convey info about past, current, future
- Signal important events, opportunities, warnings
- Trigger an action
- Confirmation of action
- Meets needs of organisation & users

Important factors in Input / Output design :
(**C**elina & **M**anisha **F**eature on **FTV**)

- **C**ontent
- **M**edia
- **F**orm
- **F**ormat
- **T**imeliness
- **V**olume

METHODS OF VALIDATING PROPOSAL

- Checklists
- Point Scoring Analysis
- Public evaluation Reports
- Benchmarking problem for vendor's proposal
- Test problems

Validation of Vendors' proposals:
(Vice-**C**hairman **M**anages **C**ompany's **P**ortfolio**)**

- **V**endor Support
- **C**ompatibility with Existing Systems
- **M**aintainability of the proposed system
- **C**ost benefits of the proposed system
- **P**erformance rating of the proposed system in relation to its cost

PHYSICAL DESIGN:

Design Principles -

- The recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria.
- Design should be based on analysis
- The software functions designed should be directly relevant to business activities.
- Design should follow standards laid down.
- Design should be modular.

PHASE -IV -Part 2:
DEVELOPMENT (PROGRAMMING TECHNIQUES AND LANGUAGES)

Objective:

To convert the specification into a functioning system.

Activities :

Application programs are written, tested and documented, conduct system testing.

Document/ Deliverable:

A fully functional and documented system.

PHASE - IV - Part 1: SYSTEM ACQUISITION

Acquisition Standards

- Ensuring security, reliability, and functionality already built into a product.
- Ensuring managers complete appropriate vendor, contract, and licensing reviews.
- Including invitations-to-tender and request for proposals,
- Establishing acquisition standards ensure functional Security, and operational requirements to be accurately identified and clearly detailed in request-for-proposals.

ADVANTAGES OF APPLICATION SOFTWARE:

- Rapid implementation
- Cost
- Quality
- Low risk

Characteristics of A Good Program Code:

- Reliability
- Robustness
- Accuracy
- Efficiency
- Usability
- Readability

Program Debugging

Debugging refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. It consists of:

- Inputting source program to the compiler,
- Letting the compiler find errors in the program,
- Correcting lines of code that are erroneous, and
- Resubmitting the corrected source program as Input to the compiler.

PHASE - V: SYSTEM TESTING

UNIT TESTING - Categories of tests that a programmer typically performs on a program unit : (**P**ayal **P**atel **F**ights **S**tuti **S**harma)

- **P**erformance Tests – Verify response time, execution time, throughput, etc.
- **P**arallel Tests – Same data in new and old, compare output
- **F**unctional Tests – Do what they are supposed to do
- **S**tress Tests – Determine stability.
- **S**tructural Tests – Examine internal processing logic

TYPES OF UNIT TESTING

- **Static Analysis Testing :**
  - Desk Check – Programmer himself
  - Structured walk-through – leads other programmer through the text
  - Code inspection – reviewed by formal committee
- **Dynamic Analysis Testing:**
  - Black Box – takes external perspective, usually functional, applicable to all levels.
  - White Box – takes internal perspective, requires programming skill, applied to unit.
  - Gray Box Testing – Combination

INTEGRATION TESTING

- Bottom-up Integration – Traditional strategy, easy to implement, The disadvantage - testing of major decision / control points deferred to a later period.
- Top-down Integrations - Starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module.
- Regression Testing - ensure that changes or corrections have not introduced new errors.

SYSTEM TESTING -

- Recovery Testing- how well application is able to recover from crashes
- Security Testing - protects data maintains functionality & existence of access controls
- Stress / Volume Testing - testing beyond normal operating capacity, often to breaking point
- Performance Testing - Compares the new system's performance with that of similar systems using well defined benchmarks

FINAL ACCEPTANCE TESTING

- **Quality Assurance Testing -** satisfies the prescribed quality standards and development process is as per organization's quality assurance methodology
- **User Acceptance Testing:**
  - Alpha Testing – performed by users within the organization.
  - Beta Testing – performed by external users

PHASE VI : SYSTEM IMPLEMENTATION **EQUIPMENT INSTALLATION** • Site Preparation • Installation of New Hardware / Software • Equipment Checkout • TRAINING PERSONNEL • System Operators Training • Users Training **CONVERSION PROCEDURE** Activities for successful conversion: (Football Players Sing Songs Always) • File conversion; • Procedure conversion • System conversion • Scheduling personnel and equipment Alternative plans in case of equipment failure **System Conversion Strategies :** • Direct Implementation / Abrupt change-over • Phased conversion • Pilot conversion Parallel running changeover	**PHASE VII - POST-IMPLEMENTATION REVIEW & MAINTENANCE** • Development Evaluation – System developed within schedule and budget. • Operation Evaluation – capable of performing their duties. • Information Evaluation – extent to which information provided is supportive of decision making	**SYSTEM MAINTENANCE** • Scheduled maintenance - Is anticipated and can be planned for • Rescue maintenance - Refers to previously undetected malfunctions that were not anticipated but require immediate solution • Corrective maintenance - fixing bugs in the code or defects found • Adaptive maintenance - adapting software to changes in the environment • Perfective maintenance – accommodating to new or changed user requirements and concerns functional enhancements • Preventive maintenance - Concerns activities aimed at increasing the system's maintainability
-OPERATION MANUALS • A cover page, a title page and copyright page; • A preface and information on how to navigate the user guide; • A contents page; • A guide on how to use at least the main functions of the system; • A troubleshooting section;	• A FAQ (Frequently Asked Questions); • Where find further help, contact details; • A glossary and an index. • Auditors' role in SDLC **The audit of systems under development can have three main objectives:** (a) to provide an opinion on Efficiency Effectiveness, and Economy (EEE) of project management;	(b) to assess the extent to which system being developed has adequate audit trails and controls to ensure integrity of data processed and stored; and (c) to assess the controls being provided for management of the system's operation.

CHAPTER 6 – AUDITING OF INFORMATION SYSTEMS

EFFECT OF COMPUTERS ON AUDIT

1. **Changes to evidence collection: (DEV-VIL)**
   - Data retention and storage
   - Audit Evidence
   - Lack of Visible output
   - Lack of a Visible audit trail
   - Absence of Input documents
   - Legal issues
2. **Changes to Evidence Evaluation**
   - System generated transactions
   - Systematic Error

Information Systems Auditing

Definition:

"IS Audit is the process of collecting and evaluating evidence to determine whether a computer system (information system) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently".

IS Audit Objectives:

Thus IS Audit objectives can be broadly divided into two categories:

(i) Asset Safeguarding Objectives:

(ii) Data Integrity Objectives:

(iii) System Effectiveness Objectives:

(iv) System Efficiency Objectives:

NEED FOR CONTROL & AUDIT OF IS:

Factors influencing an organization toward control and audit of computers

- Organisational Costs of Data Loss
- Incorrect Decision Making
- Costs of Computer Abuse
- Value of Computer Hardware, Software and Personnel
- Maintenance of Privacy
- Controlled evolution of computer use.

CATEGORIES OF IS AUDITS

- Management of IT and Enterprise Architecture
- Information Processing Facilities
- Systems and Applications
- Systems Development
- Telecommunications, Intranets and
- Extranets

Skill set of IS Auditor

The set of skills that is generally expected of an IS auditor include:

- Sound knowledge of business operations, practices and compliance requirements,
- Should possess the requisite professional technical qualification and certifications,
- An good understanding of information Risks and Controls,
- Knowledge of IT strategies, policy and procedure controls,
- Ability to understand technical and manual controls relating to business continuity, and
- Good knowledge of Professional Standards and Best practices of IT controls and security

FUNCTIONS OF IS AUDITOR: IS Auditor reviews risk related to IT systems, like:

- Inadequate information security
- Inefficient use of corporate resources, or poor governance
- Ineffective IT strategies, policies and practices
- IT-related frauds

THE IS AUDIT PROCESS

- Assessment of internal controls within the IS environment to assure validity, reliability, and security information.
- Assessment of the efficiency and effectiveness of the IS environment in economic terms.

STEPS IN INFORMATION TECHNOLOGY AUDIT:

- Scoping and pre-audit survey
- Planning and preparation
- Fieldwork
- Analysis
- Reporting

Audit Standards & Best Practices

(a) ISACA – Information Systems Audit and Control Association

Is a global leader in information governance, control, security and audit.

ISACA developed the following to assist IS auditor while carrying out an IS audit.

IS auditing standards:

16 auditing standards which defines the mandatory requirements for IS auditing and reporting.

IS auditing guidelines:

39 auditing guidelines which provide a guideline in applying IS auditing standards.

IS auditing procedures:

11 IS auditing procedures which provide examples of procedure an IS auditor need to follow while conducting IS audit for complying with IS auditing standards.

(b) Control Objectives For Information Related Technology (COBIT)

The Information Systems Audit and control Foundation (ISACF) developed the Control Objectives for Information and related Technology (COBIT). COBIT framework is detailed in chapter no. 1

(c) ISO 27001: ✓ Is international best practice and certification standard for an Information Security Management System (ISMS). ✓ Is a systematic approach to manage Information security in an IS environment **(d) IIA – The Institute of Internal Auditors** ✓ IIA issued Global Technology Audit Guide (GTAG) GTAG provides: • Management of organisation about information technology management, control, and security and • IS auditors with guidance on different information technology associated risks and recommended practices. **(e) Standards on Internal Audit issued by ICAI:** ICAI has issued various standards; the details are given in the Study Material of Auditing paper. **(f) ITIL: The Information Technology Infrastructure Library** is a set of practices for IT Service Management (ITSM) focuses on aligning IT services with the needs of business.	**CONCURRENT / CONTINUOUS AUDIT - Types of Audit Tools:** (**S**onakshi **I**s **S**mart and **C**ool) ▪ **Snapshots** • Enable tracing a transaction in a computerised system. • The snapshot software is built into the system at those points where material processing occurs • It takes images of the flow of any transaction as it moves through the application. • These images can be utilised to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.	▪ **Integrated Test Facility (ITF)** • Involves the creation of a dummy entity in the application system files and • Processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness.
▪ **System Control Audit Review File (SCARF)** • Involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. • The information collected is written onto a special audit file- the SCARF master files.	✓ Auditors might use SCARF to collect the following types of information : - Application system errors - Policy and procedural variances - System exception - Statistical sample - Snapshots and extended records - Performance measurement	• **Continuous and Intermittent Simulation (CIS)** - Used to trap exceptions whenever the application system uses a database management system by replicating or simulating the application system processing. - Every update to the database that arises from processing the selected transaction will be checked by CIS to determine whether discrepancies exist between the results it produces and those the application system produces.

Advantages of Continuous Audit Techniques

- Timely, comprehensive and detailed auditing
- Surprise test capability
- Information to system staff on meeting of objectives
- Training for new users. Disadvantages
- Auditors should be able obtain resources required from organisation to support it
- More likely to be used if auditors are involved in the development work of a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use it effectively and efficiently.
- It is more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- It won' be effective if the application system is not relatively stable.

AUDIT TRAILS

- ✓ Are logs that can be designed to record activity at the system, application, and user level.
- ✓ Maintain a chronological record of all events that have occurred in a system.
- ✓ Provide an important detective control to help accomplish security policy objectives.

- Objectives: (Revenge Against Defaulters)
  - Reconstructing Events
  - Personal Accountability
  - Detecting Unauthorized Access

General Controls

These controls apply to a wide range of exposures that systematically

threaten the integrity of all applications processed within the Computer

Based Information System (CBIS) environment.

Can be further subdivided under following headings:

1. O/S Controls

Log-in Procedures

Access Token

Access Control List

Discretionary Access control

2. Data Management Controls

I. Access Controls

User Access

Biometric Controls

Encryption of Data stored in Databases

II. Backup Controls

Dual Recording of Data

Periodic Dumping of Data

Logging Input Transactions

Logging Changes to Data

3. Org. Structure Controls

Segregate maker from checker

Segregate asset recorder from physical asset keeper

Improve Documentation

Deny programmer access to prod. env.

4. System Development Controls

System Authentication Activities

User Specification Activities

Technical Design Activities

Internal Auditor's Participation

Program Testing

User Test & Acceptance Procedures

5. System Maintenance Controls

Same Treatment as SYSTEMS DEVELOPMENT

6. Computer Center & Security Controls

I. Physical Security

Fire Damage

Water Damage

Power Supply Variation

Pollution Damage

II. Software & Data

Security, Authorisations

Passwords & PINs

SOD, Frequent Audits

III Data Communication Security

Audit trail of Network activ., Encryption,

Approved network protocols, Terminal locks

7. Internet & Intranet Controls

Component Failure

Subversive threats

Firewall

Encryption

Recording of Transaction log

Call Back Devises

8. Personal Computer Controls

Physically lock the system.

Log equipment shifting.

Centralised purchase of h/w.

Stds. for developing, testing..

Anti-malware software

Application Controls:

Application controls deal with exposures within specific applications, such as payroll, purchases, and cash disbursements systems.

1. Input Controls

(a) Source Document Controls
- Pre-numbered
- Sequence
- Periodic audit

(b) Data Coding Controls

(c) Validation Controls
- Field Interrogation
  - Limit Check
  - Picture Check
  - Valid Code Check
  - Check Digit
  - Arithmetic Check
  - Cross Check
- Record Interrogation
  - Reasonableness Check
  - Valid Sign
  - Sequence Check
- File Interrogation
  - Version Usage
  - Internal & External Labeling
  - Before and after Image Logging
  - File updating and Maintenance Authorisation
  - Parity Check

2. Processing Controls

Run-to-run totals
Reasonableness verification
Edit Checks
Field Initialisation
Exception Reports

3. Output

Storage and Logging of sensitive, critical forms
Logging of output program executions
Spooling / Queuing
Controls over printing
Report distribution & collection controls
Retention controls

Audit of Application Security Controls

- Objective is to establish whether the application security controls are operating effectively to protect the confidentiality, integrity and availability of information.

A layered approach is used based on the functions and approach of each layer.

(i) Operational Layer:

The operational layer audit issues include:

- User Accounts and Access Rights:
- The objective is to assure that users and applications should be uniquely identifiable.
- Password Controls:
- Check whether there are applications where password controls are weak.
- Segregation of Duties:
- SOD prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and custody of assets to separate individuals. Auditor needs to check that there is no violation of above principle.

(ii) Tactical Layer:

At the tactical layer, security administration is put in place. This includes:

- Timely updates to user profiles, like creating/deleting and changing of user accounts. Auditor needs to check that any change to user rights is a formal process including approval from manager of the employee.
- IT Risk Management:
- It includes the following activities:
- Assessing risk over key application controls;
- Conducting a regular security awareness programme on application user;
- Enabling application users to perform a self-assessment;
- Reviewing application patches;
- Updating antivirus software
- Interface Security:
- This relates to application interfaced with another application in an organization.
- Audit Logging and Monitoring:
- May be done on an exception reporting basis.

(iii) Strategic Layer:

Top management takes action including drawing up security policy, security training, security guideline and reporting, a comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security.

Auditor needs to check the presence of the above.

CHAPTER 7 – INFORMATION TECHNOLOGY REGULATORY ISSUES

(Only ISO / ICE 27001 & ITIL)

ISO / IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems – Requirements

- Is international best practice and certification standard for an Information Security Management System (ISMS).
- Is a systematic approach to manage Information security in an IS environment
- Encompasses people, technology and processes.
- Defines how to organise information security in any kind of organization, profit or non-profit, private or state-owned, small or large.
- Enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organisation as defined policies and procedures.

Four Phases of ISMS – (See Chart)

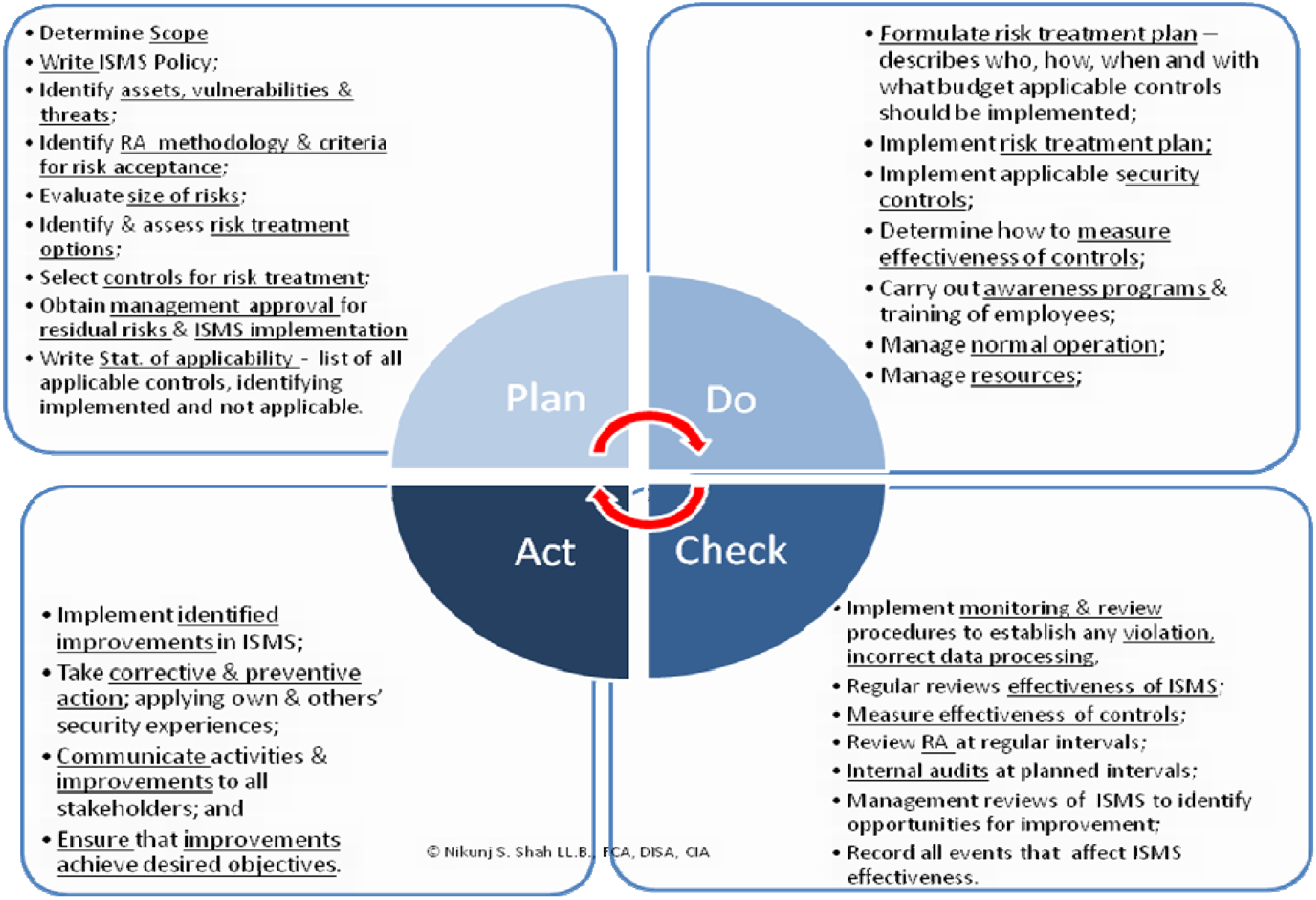
Should be continuously implemented in order to minimise risks. These include

The Plan Phase – Serves to plan basic organisation of IS by setting objectives for IS & choosing appropriate security controls (from a catalogue of 133 possible controls).

The Do Phase – Includes carrying out everything that was planned during previous phase.

The Check Phase – Monitors functioning of ISMS through various "channels", and check whether results meet set objectives.

The Act Phase – Improve everything that was identified as non-compliant in previous phase.


• Determine Scope
• Write ISMS Policy;
• Identify assets, vulnerabilities & threats;
• Identify RA methodology & criteria for risk acceptance;
• Evaluate size of risks;
• Identify & assess risk treatment options;
• Select controls for risk treatment;
• Obtain management approval for residual risks & ISMS implementation
• Write Stat. of applicability - list of all applicable controls, identifying implemented and not applicable.
Plan
• Formulate risk treatment plan – describes who, how, when and with what budget applicable controls should be implemented;
• Implement risk treatment plan;
• Implement applicable security controls;
• Determine how to measure effectiveness of controls;
• Carry out awareness programs & training of employees;
• Manage normal operation;
• Manage resources;
Do
Act
• Implement identified improvements in ISMS;
• Take corrective & preventive action; applying own & others' security experiences;
• Communicate activities & improvements to all stakeholders; and
• Ensure that improvements achieve desired objectives.
Check
• Implement monitoring & review procedures to establish any violation, incorrect data processing,
• Regular reviews effectiveness of ISMS;
• Measure effectiveness of controls;
• Review RA at regular intervals;
• Internal audits at planned intervals;
• Management reviews of ISMS to identify opportunities for improvement;
• Record all events that affect ISMS effectiveness.
© Nikunj S. Shah LL.B., FCA, DISA, CIA

ITIL (IT Infrastructure Library): is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business.

Stresses running IT like a business.

ITIL describes procedures, tasks and checklists used by an organization for establishing a minimum level of competency for ITSM.

ITIL v3 2011 edition published in a series of five core publications, each covering an ITSM lifecycle stage.

1. **Service Strategy –** Deals with:
   i. Strategic Analysis - What are we going to provide?
   ii. Plan - Can we afford it?
   iii. Position - How do we gain competitive advantage?
   iv. Implementation - Can we provide enough of it?
   v. Perspective – What would be vision, mission and strategic objectives?

   Topics Include:
   i. Define Markets – Internal & External
   ii. Develop the Offerings – Service Asset, Service Catalog
   iii. Prepare for Execution - Implementation Strategy
   iv. Identify, select & prioritize opportunities

2. **Service Design –**
   i. Translates strategic plans & objectives into service assets
   ii. It includes design principles and methods for converting strategic objectives into portfolios of services and service assets.
   iii. Not limited to new services and includes the changes and improvements required to maintain or increase value to customers over the lifecycle of services.
   iv. Creates Design - How are we going to build it?
   v. Specs for execution - How are we going to test and deploy it?

3. **Service Transition –** Provides guidance on:
   i. Development and improvement of capabilities for transitioning new and changed services into operations.
   ii. Realising Strategy encoded in Design through Operation, whilst controlling the risks of failure and disruption
   iii. Managing complexity of changes to prevent undesired consequences whilst permitting for innovation.
   iv. Transferring control of services between customers & service providers.

4. **Service Operation -** Provides guidance on:
   i. Management of a service through its day-to-day production life.
   ii. Supporting operations by new models and architectures such as shared services, utility computing, web services, and mobile commerce.
   iii. Achieving efficiency & effectiveness in delivery & support of services to ensure value for customer & service provider.

5. **Continual Service Improvement -** Provides guidance on:
   i. Measurement of service performance through the service life-cycle,
   ii. Suggesting improvements to ensure that service delivers maximum benefit.
   iii. Creating & maintaining value for customers through improved design, introduction, and operation of services.
   iv. Linking improvement efforts and outcomes with service strategy, design, and transition, focusing on increasing the efficiency, maximizing the effectiveness and optimizing cost of services and the underlying IT Service Management processes.

CHAPTER 8 – EMERGING TECHNOLOGIES

Cloud Computing:

- ✓ Means use of computing resources as a service through networks, typically the Internet.
- ✓ Computation done through the Internet.
- ✓ Is a combination of software and hardware based computing resources delivered as a networked service.
- ✓ Is platform independent
- ✓ The consumers may not own the infrastructure, software, or platform
- ✓ End users may not need to care about how servers and networks are maintained in the cloud, and can access multiple servers anywhere on the globe without knowing 'which ones and where they are located'.
- ✓ Applications and resources can be accessed using a simple front-end interface such as a Web browser.
- ✓ Allows companies to scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software.
- ✓ Service consumers use 'what they need on the Internet' and pay only for 'what they use'.
- √ The best example is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.

Grid Computing:

Cloud computing evolved from grid computing and provides on-demand resource provisioning.

Grid computing requires the use of software that can divide and carve out pieces of a programs one large system image to several thousand computers.

Thus if one piece of the software on a node fails, other pieces of the software on other nodes may fail.

- This is alleviated if that component has a failover component on another node

B. Similarities and Differences:

- Scalability - both are scalable.
- Both involve multi tenancy and multitasking
- Both provide Service-Level Agreements (SLAs)
- Grid – Suitable only for large data / computationally intensive operations

Pertinent Issues:

- Threshold Policy:
- Interoperability:
- Environment Friendly Cloud Computing:
- Hidden costs
- Unexpected behavior
- Security issues
- Application development in cloud

Goals of Cloud Computing:

The core goals of utilizing a cloud-based IT ecosystem are to pool available resources together into a highly efficient infrastructure whose costs are aligned with what resources are actually used but to the services accessible and available from anywhere at any time.

To meet the requirements, some of the pertinent objectives in order to achieve the goals are as follows:

- To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;
- To access services and data from anywhere at any time;
- To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- To consolidate IT infrastructure into a more integrated and manageable environment;
- To reduce costs related to IT energy/power consumption;
- To enable or improve "Anywhere Access" (AA) for ever increasing users; and
- To enable rapidly provision resources as needed.

Cloud Computing Architecture

A cloud computing architecture consists of a front end and a back end.

They connect to each other through a network, usually the Internet.

- **Front End Architecture:**

  Client's devices (or computer network) and some applications needed for accessing the cloud computing system e.g. some existing web browsers or some unique applications which provide network access to its clients.

- **Back End Architecture:**

  Various computer machines, data storage systems and servers

  Web application program

  An application server dedicated for each service.

  A central server for administering the whole system & for monitoring client's demand as well as traffic.

  Some set of rules, called protocols.

  Middleware – which allows computers connected on networks to communicate with each other.

  Huge storage space

  Storage devices

  Redundant back-up copy of all the data of its client's.

Cloud Computing Environment:

(a) Public Clouds:

This environment can be used by the general public.

Are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis.

Advantages:

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.

Limitations - is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen.

(b) Private Clouds:

- ✓ Also called internal clouds, these reside within boundaries of an organization and used exclusively for organization's benefits.
- ✓ Are built primarily by IT departments within enterprises

Advantages:

Improved average server utilization; allow usage

- of low-cost servers and hardware while providing higher efficiencies; thus reducing the costs that a greater number of servers would otherwise entail.
- Reduced operations costs and administrative overheads.

Limitation:

IT teams in the organization may have to invest in buying, building and managing the clouds independently.

(c) Hybrid Clouds:

Is combination of both at least one private (internal) and at least one public (external) cloud computing environments – usually, consisting of infrastructure, platforms and applications.

Cloud Computing Models

(a) Infrastructure as a Service (IaaS):

IaaS providers offer computers, more often virtual machines and other resources as service.

It provides the infrastructure / storage required to host the services.

To deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure.

(b) Platform as a Service (PaaS):

Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server.

Cloud users can develop and run their software solutions on a cloud platform without the cost and complexity of acquiring and managing the underlying hardware /software layers.

It gives us the platform to create, edit, run and manage the application programs we want.

All the development tools are provided.

(c) Software as a Service (SaaS):

Provides users to access large variety of applications over internets that are hosted on service provider's infrastructure.

(d) Network as a Service (NaaS):

Provides network/transport connecting services to the cloud user.

Optimizes resource allocation by considering network and computing resources as a whole.

(e) Communication as a Service (CaaS):

Is an outsourced enterprise communication solution that can be leased from a single vendor.

The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS).

It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis

Characteristics of Cloud Computing:	***Advantages of Cloud Computing:***	***Challenges relating to Cloud Computing:***
• High Scalability: • Agility: • High Availability and Reliability: • Multi-sharing: • Services in Pay-Per-Use Mode: • Virtualization: • Performance: • Maintenance:	• Cost Efficiency: • Almost Unlimited Storage: • Backup and Recovery: • Automatic Software Integration: • Easy Access to Information: • *Quick Deployment:*	• **Confidentiality:** Prevention of the unauthorized disclosure. This challenge can be addressed with the use of encryption and physical isolation, data can be kept secret. • **Integrity:** Refers to the prevention of unauthorized modification Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. Also, employ cryptographic hash function. • **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the **data backup** through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). • **Governance:** There is a need of governance model, which controls the standards, procedures and policies of the organisation. • **Trust:** Various clients oriented studies reveal that Cloud has still failed to build trust between the client and service provider. • **Legal Issues and Compliance:** It is responsibility of the cloud suppliers that they are protecting the data and supplying to the customer in a very secure and legal way but one of the major troubles with laws is that laws vary from place to place.

- **Privacy:**
  The Cloud should be designed in such a way that it decreases the privacy risk.
- **Audit:**
  Auditing is type of checking that 'what is happening in the Cloud environment'. The context of use of Cloud, time consuming audits seriously detains a key gain of Cloud agility.
- **Data Stealing:**
  In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing.
- **Architecture:**
  In the architecture of Cloud computing models, there should be a control over the security and privacy of the system.
- **Identity Management and Access control:**
  The key critical success factor for Cloud providers is to have a robust federated identity management architecture and strategy internal in the organization.
- **Incident Response:**
  The Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.
- **Software Isolation:**
  In Cloud service provider's multi-tenant software architecture, organisations must understand virtualization and other logical isolation techniques and evaluate the risks required for the organisation.
- **Application Security:**
  Infected applications need to be monitored and recovered by the Cloud security drivers.

Mobile Computing

It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. This proves to be the solution of the biggest problem of business people on the move i.e. mobility.

Mobile Computing Services

Mobile Computing Services allow mobile workforces to access a full range of corporate services and information from anywhere, at any time and it improves the productivity of a mobile workforce by connecting them to corporate information systems and by automating paper-based processes.

Mobile Computing Benefits

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties / service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.
- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

BYOD (Bring Your Own Device):

Refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. This has led to an increase in employee's satisfaction and also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

Emerging BYOD Threats:

- **Network Risks:**
  As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network.
- **Device Risks:**
  Data lost from stolen or lost devices ranks as the top security threats
- **Application Risks:**
  It is normally exemplified and hidden in 'Application Viruses and Malware'. Organizations are not clear in deciding that '**who is responsible for device security – the organization or the user'**.
- **Implementation Risks:**
  It is normally exemplified and hidden in **Weak BYOD Policy'**. T**he absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse.**

Web 2.0

- ✓ The term describes a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online.
- ✓ Refers to transition from static HTML Web pages to a more dynamic Web
- ✓ Is more organized and is based on serving Web applications to users.
- ✓ Includes open communication with an emphasis on Web-based communities of users, and more open sharing of information.
- ✓ Tries to tap the power of humans connected electronically through its new ways at looking at social collaboration. This is one of the commonalities between social networks and Web 2.0 - both have people as their fulcrum.
- ✓ The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner.
- ✓ The power of Web 2.0 is the creation of new relationships between collaborators and information.
- ✓ In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mashups, and Tagging.
- ✓ Combined with other such concepts, Web 2.0 provides an ideal platform for implementing and helping Social Networks to grow.

Components of Web 2.0 for Social Networks

- **Communities:**
  online space formed by a group of individuals to share their thoughts, ideas
- **Blogging:**
  Blogs **give the users** of a Social Network the **freedom to express their thoughts** in a free form basis and helping generation and discussion of topics.
- **Wikis:**
  A Wiki is a **set of co-related pages on a particular subject and allow users to share content**.
- **Folksonomy:**
  A feature where users can **tag their content online and this enables other to easily find and view such other content**.
- **File Sharing / Podcasting:**
  Helps users to **send their media files and related content online**
- **Mashups:**
  This facility allows people to congregate services from multiple vendors to create completely new services.

Types of Social Networks

- **Social Contact Networks:** Formed to keep contact with friends and family.
- **Study Circles:** Social networks dedicated for students
- **Social Networks for Specialist Groups:** Designed for core field workers like doctors, scientists, engineers, members of the corporate industries. e.g. - LinkedIn.
- **Networks for Fine Arts:** Dedicated to people linked with music, painting and related arts
- **Police and Military Networks:** Operate much like social networks on a private domain due to the confidentiality of information.
- **Sporting Networks:** Dedicated to people of the sporting fraternity
- **Mixed Networks:** Have a subscription of people from all the above groups
- **Social Networks for the 'inventors':** Social networks for the people who have invented the concept of social networks.
- **Shopping and Utility Service Networks:** Try to analyze the social behaviour and send related information for the same to respective marts and stores.
- **Others:** Some of these networks die out very fast due to lack of constructive sustenance thoughts while others finally migrate to a more specialist network.

Benefits and Challenges for Social Networks using Web 2.0:

Benefits:

Provides platform where users need not to worry about the implementation or underlying technology

Very affordable cost.

Blogging is easy - no new knowledge skills are required.

People centric activities - Thus adaptation is very fast.

People are coming much closer to another

Social and geographical boundaries are being reduced at lightning speed.

Challenges:

Data security and privacy and is the biggest concern – as there are no centrally mandated administrative services to take care of such aspects.

Privacy of individual users also arises and can create huge problem if malicious users somehow manage to perpetuate the social networks.

A majority of the social networks are offline, and for bringing these under the purview of online social networks, a lot of education and advertising needs to be done.

Green IT

Refers to the study and practice of establishing / using computers and IT resources in a more efficient, environmentally friendly and responsible way.

Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle.

Include implementation of energy-efficient CPUs, servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

One of the earliest initiatives toward green computing in the United States was the voluntary labeling program known as Energy Star.

Some of such steps for Green IT include the following:

- Power-down the CPU and all peripherals during extended periods of inactivity.
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.
- Power-up and power-down energy-intensive peripherals such as laser printers according to need.
- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
- Use notebook computers rather than desktop computers whenever possible.
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity.
- Minimize the use of paper and properly recycle waste paper.
- Dispose of e-waste according to central, state and local regulations.
- Employ alternative energy sources for computing workstations, servers, networks and data centres.

Green IT Best Practices

From the experience of practicing professionals, there are a range of well identified best-practices. A few of those for assurance purposes are listed as follows:

- Involving stakeholders on campus yields policies and green IT initiatives more likely to be embraced by the campus community.
- Partnering takes advantage of existing efforts and ensures wider reach and more effective use of limited resources.
- Guidelines for using the best practices simplify adaption of green IT by campus users and encourage them to consider green computing practices the norm.
- On-going communication about and campus commitment to green IT best practices to produce notable results.