# ISCA *(The Compressed Love)* CA FINAL

***8 CHAPTERS → 114 MARKS → IN 78 PAGES → COVERED 100% SM & PM***
***ALL PM CONTENT HIGHLIGHTED WITH PURPLE COLOUR***
***REMAINING CONTENT COVERED IN BLACK FONT***
***TO LEARN QUICKLY → EVERYTHING EXPLAINED IN TREE STRUCTURE WITH ADEQUATE HEADING***


***By Rajveer Singh***

***You can give me your valuable feedback through***
***Email → rajveer.an.indian@gmail.com***
***WhatsApp → +919570143130***

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

**Governance:** The term "**Governance**" is derived from Greek word meaning "to steer". A governance system typically refers to *means & mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance & performance, in order to satisfy specific enterprise objectives.*

**Benefits of Governance**

- Achieving enterprise objectives by ensuring that each element of mission & strategy are assigned & managed with transparent decisions rights & accountability framework;
- Defining & encouraging effective use of IT and execution of IT outsourcing arrangements;
- Implementing & integrating desired business processes into the enterprise;
- Providing stability & overcoming the limitations of organizational structure;
- Improving customer satisfaction, business & internal relationships, and reducing internal territorial strife by implementing a holistic IT governance framework; and
- Enabling effective & strategically aligned IT decision making in tune with business.

*(Note – Based on above, IT is integral part of Governance. IT Governance is a subset of Enterprise Governance.)*

**Enterprise Governance** can be defined as *'The set of responsibilities & practices exercised by Board & Executive Management of an enterprise. The goal is to provide strategic direction to ensure that objectives are achieved, ascertaining that risks are managed appropriately and verifying that enterprise's resources are used responsibly.'*

**Enterprise Governance has two dimensions:** *(Enterprise must balance these dimensions so as to meet the Stakeholders requirement & to Ensure long term success.)*

**Corporate Governance (i.e. Conformance):** *(Accountability & Assurance)*

***Corporate Governance** is the system by which a company or enterprise is directed & controlled to achieve the objective of increasing shareholder value by enhancing economic performance.* Corporate governance refers to the structures & processes for the direction & control of companies.

**Good corporate governance** contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business to protect shareholders' interest.

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 & compliance with laws & standards. It guide companies to achieve their business objectives without compromising the shareholders' interest.

Regulatory requirements & standards generally address this dimension with compliance being subject to assurance and/or audit. There are established oversight mechanisms for the board to ensure that good corporate governance processes are effective. E.g. Committees composed of Independent NED, AC. Other committees like NRC. **Sarbanes Oxley Act of US** & Clause 49 listing requirements of SEBI.

**Business Governance (i.e. Performance):** *(Value Creation & Resource Utilization)*

*The **Business Governance** is business oriented thus pro-active in its approach & takes a forward looking view. This dimension focuses on strategy & value creation with the objective of helping the board to make strategic decisions, understand its risk appetite & its key performance drivers.*

This dimension does not governed by any standard & assurance as this is specific to enterprise goals & varies based on the mechanism to achieve them.

* Conformance dimension is monitored by AC and Performance dimension in terms of overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism.

**Some of Best practices of corporate governance:**

- Clear assignment of responsibilities & decision-making authorities;
- Establishment of a mechanism for interaction & cooperation among board of directors, senior management & the auditors;
- Implementing strong IC systems;
- Monitoring risk exposures where conflicts of interest are likely to be particularly great. (E.g. Related party transactions);
- Financial & managerial incentives to senior management & employees offered in an appropriate manner; &
- Appropriate information flows internally (e.g. Internal Audit Report to BOD) & externally (e.g. XBRL to MCA).

*"**IT Governance** is system by which IT activities in a company / enterprise are directed & controlled to achieve business objectives with ultimate objective of meeting stakeholder needs".*

Hence, overall objective of IT Governance is very much similar to Corporate Governance but IT Governance focuses on IT. IT Governance= sub-set of Corporate/Enterprise Governance. Although, terms IT Governance & Governance of Enterprise IT (GEIT) are used inter-changeably, the term GEIT is more macro & broader in its scope of coverage.

*IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.*

**Benefits of IT Governance**

- Increased *value* delivered through enterprise IT;
- Increased *user satisfaction*;
- Improved *agility* in supporting business needs;
- Better *cost performance*;
- *Improved management & mitigation of IT-related business risk*;
- IT becoming an *enabler for change rather than an inhibitor*;
- *Transparency & understanding of IT's contribution* to business;
- *Compliance* with relevant laws, regulations & policies; and
- *Optimal utilization of IT resources*.

**Key practices to determine status of IT Governance**

- Who makes directing, controlling & executing decisions?
- How decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How governance results are monitored & improved?

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

**Governance of Enterprise IT (GEIT)** is a sub-set of corporate governance & facilitates implementation of framework of IS controls within an enterprise encompassing all key areas.

**Objectives**

- To analyze & articulate the requirements for GEIT, &
- To put in place & maintain effective enabling structures, processes & practices, with clarity of responsibilities & authority to achieve enterprise's mission, goals & objectives.

**Benefits of GEIT**

- Provides consistent approach integrated & aligned with enterprise governance approach.
- Ensures → IT-related decisions are made in line with enterprise's strategies & objectives.
- Ensures → IT-related processes are overseen effectively & transparently.
- Compliance with law.
- Ensures → governance requirements for board are met.

**Key Governance Practices of GEIT**

- **Evaluate the Governance System:** Continually identify & engage with enterprise's stakeholders, document understanding of the requirements, and make judgment on current & future design of GEIT;
- **Direct the Governance System:** Inform management and obtain their support & commitment. Guide structures, processes & practices for GEIT in line with agreed governance design principles, decision-making models & authority levels.
- **Monitor the Governance System:** Monitor effectiveness & performance of GEIT. Assess whether governance system & implemented mechanisms are operating effectively.

**ENTERPRISE RISK MANAGEMENT (ERM)** *(SOX require strong IC & COSO has given the framework for implementing IC i.e. How to implement IC)*

In implementing controls, it is important to adapt a holistic & comprehensive approach. Hence, it should consider business objectives, processes, organization structure, technology deployed & the risk appetite. Based on these, overall risk management strategy has to be adapted, which should be designed & promoted by top management & implemented at all levels of enterprise operations. The **Sarbanes Oxley Act (SOX)** in the US, which focuses on implementation & review of IC relating to financial audit, highlights the importance of evaluating the risks, security & controls related to FS. SOX uses **COSO** as one of the important guidelines for implementing risk management & internal controls.

"ERM is a ***process***, effected by an entity's board of directors, management & other personnel, applied in strategy setting & 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*."

**INTERNAL CONTROLS**

**[WHY: To make FS true & fair i.e. FS will be as per GAAP. Where management will ensure FS is made as per accounting principles.]**

"Internal Control over financial reporting" is "process designed by company's top management to provide reasonable assurance regarding reliability of FR & preparation of FS as per GAAP and includes those policies & procedures that:

- Pertain to *maintenance of detailed records* that accurately & fairly reflect *transactions & dispositions of assets* of the company;
- Provide *reasonable assurance* that transactions are recorded as necessary to permit *preparation of FS as per GAAP* and *receipts & expenditures* of the company made only in accordance with *authorizations of management & directors* of the company;
- Provide reasonable assurance regarding *prevention or timely detection of unauthorized acquisition, use or disposition of company's assets* having material effect on FS.

Company's Annual Report must include "An IC Report of Management" that contains:

- A *statement of management's responsibility* for establishing & maintaining adequate IC over FR for the company;
- A *statement identifying the framework used by management* to conduct required evaluation of the effectiveness of company's IC over FR;
- *Management's assessment of effectiveness of the Company's IC* over FR at the year-end including a statement as to whether or not the Company's IC over FR is effective, disclosing weakness, if any. &
- A *statement that Registered Public Accounting Firm that audited the FS* of the company has *issued an attestation report on Management's Assessment of Company's IC over FR*."

**(a) Responsibility for Implementing IC:** SOX made major changes in IC by holding CEOs & CFOs personally & criminally liable for the quality & effectiveness of their Organization's IC. Part of the process is to attest that Organization's IC are effective. IC can be expected to provide only a reasonable assurance, not an absolute assurance. An organization must ensure that its FS comply with **Financial Accounting Standards (FAS)** & **International Accounting Standards (IAS)** or local rules.

**(b) COSO (Committee of Sponsoring Organizations): It is standard of Internal Control** *(Stepwise)*
**Internal Controls as per COSO:** In Computerised Environment, goals of asset safeguarding, data integrity, system efficiency & system effectiveness can be achieved only if organization's management sets up a system of IC.
According to COSO, IC is comprised of five interrelated components:

- **Control Environment:** For each business process, an organization needs to develop & maintain a control environment including *categorizing the criticality & materiality of each business process and the owner of the business process*.
- **Risk Assessment:** Each business process comes with various risks. A control environment must include *an assessment of risks associated with each business process*.
- **Control Activities:** Control activities must be developed *to manage, mitigate & reduce risks associated with each business process*. It is unrealistic to expect to eliminate risks completely.
- **Information & Communication:** *Control activities are associated with information & communication systems* of the *entity*. These enable an organization to capture & exchange information needed to conduct, manage & control its business processes.
- **Monitoring:** IC process must be continuously monitored *& modifications to be made as warranted by changing conditions.*

**(c) Clause 49** of listing agreements issued by SEBI in India is similar to SOX regulation & mandates Implementation of ERM & IC and holds Senior Management legally responsible for such implementation. Further, it also provides for certification of these aspects by external auditors.

Note: COSO & COBIT used together as internationally best practices framework for complying with SOX.

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

**Steering Committee → (Member = Member of BOD + Head of all Dept. + Auditor + IT Experts)**

***(WHAT – Formed by Senior Magm. to monitor IT Department)***

Senior management may appoint a high-level committee, called IT Steering Committee, led by Member of BOD and Head of all departments including Audit & IT department.

To provide overall direction to deployment of IT & IS in the enterprises. They ensure that IT Deployment is in tune with enterprise business goals & objectives.

The role & responsibility of IT Steering Committee & its members must be documented & approved by senior management.

**Key Functions: ----------→**

- To ensure that **long & short-range plans of IT department are in tune** with enterprise goals & objectives;
- To **establish size & scope** of IT function and **sets priorities** within the scope;
- To review & approve major **IT deployment projects** in all their stages;
- To approve & monitor **key projects** (e.g. by measuring ROI of IT projects);
- To review status of **IS plans, budgets & overall IT performance**;
- To review & approve **standards, policies & procedures**;
- To make decisions on all **key aspects of IT deployment & 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 Board of Directors on **IT activities on a regular basis**.

**Asset:** *Asset can be defined as something of value to org.* They are not easily replaceable without cost, skill, time, resources. Without which org. may suffer loss. E.g., information in electronic / physical form, software systems, employees, etc.

**Vulnerability:** *Vulnerability is weakness in the system safeguards that exposes the system to threats.* It may be weakness in information system, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. E.g. Poor access control, Leaving door unlocked, Short passwords, etc.

Simply, Vulnerability can be referred as weakness of the software, which can be exploited by the attackers. Vulnerabilities can originate from flaws on software's design, defects in its implementation, or problems in its operation.

**Threat:** Any entity, circumstance, or event with potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. *A threat is an action, event or condition where there is a compromise in the system, its quality & ability to inflict harm to the organization.*

**Exploit:** An exploit is the way or tool by which an attacker uses a vulnerability to cause damage to the target system.

**Exposure:** *It is extent of loss the organization has to face when a risk materializes.* It is not just the immediate impact, but the real harm that occurs in long run.

E.g. - loss of business, failure to perform system's mission, loss of reputation, violation of privacy, & loss of resources etc.

**Likelihood of threat:** *It is estimation of the probability that the threat will succeed in achieving an undesirable event.* The presence & strengths of threats as well as effectiveness of safeguards must be considered while assessing likelihood of the threat occurring.

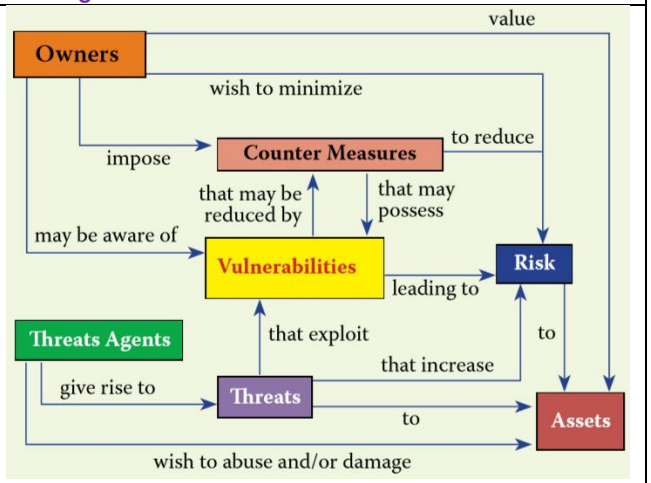
**Attack:** *An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability.* In software terms, an attack is a malicious intentional act, usually an external act that has intent of exploiting vulnerability in the targeted software or system.

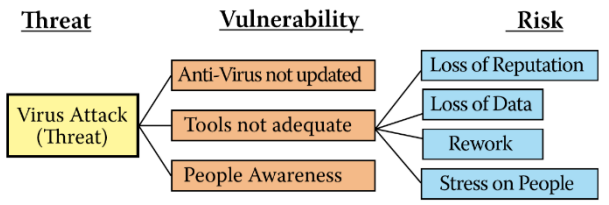
It is a set of actions designed to compromise **CIA**. Simply, it is the act of trying to defeat IS safeguards.

**Risk:** *Risk can be defined as potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset.* Risk analysis is the process of identifying security risks & determining their magnitude & impact on an org.

Risk assessment includes:

- Identification of threats & vulnerabilities;
- Potential impact or magnitude of harm to enterprise operations or enterprise assets when an identified vulnerability be exploited by a threat;
- Identification & analysis of security controls for IS.




**Counter Measure:** *An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure.*

E.g. 'spoofing the user identity', has 2 counter measures:

- Strong authentication protocols to validate users; and
- Passwords should not be stored in configuration files instead some secure mechanism should be used.

**Residual Risk:** Any risk still remaining after the counter measures are analyzed & implemented is called **Residual Risk**. An organization's management should consider: acceptance of residual risk & selection of safeguards. Even when safeguards are applied, there is probably going to be some residual risk. The risk can be minimized, but it cannot be eliminated. Residual risk must be kept at a minimal, acceptable level.

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

## RISK MANAGEMENT

*Enterprise Risk Management & IT Risk Management are key components of an effective IT governance structure of any enterprise. IT governance has to be an integral part of overall corporate risk management efforts so that appropriate risk mitigation strategies are implemented based on the enterprise risk appetite. Risk assessment approach considers impact of IS risk & different types of risks and regularly communicates the status of residual risks to key stakeholders so that appropriate action is taken to manage the IT risk profile.*

### Information Systems Risks & Risk Management

- Numerous changes in IT & its operating environment and regulatory requirement emphasize the needs to better manage & control IT related risks.
- Risk refers to possibility of something adverse happening, resulting in potential loss/exposure.
- Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level & maintaining that level of risk.
- Any IS based on IT has its inherent risks which cannot be eliminated but can be mitigated by appropriate security.
- This security has to be implemented as per required control system envisaged by the management.
- Auditors are required to evaluate whether the available controls are adequate & appropriate to mitigate the risks.
- If controls are unavailable or inadequate or inappropriate, then it should be reported to auditee management with appropriate recommendations to mitigate them.
- IT risk are mitigated by providing appropriate & adequate IS Security.
- IS security is defined as "procedures & practices to assure that computer facilities are available at all required times, that data is processed completely & efficiently and access to data in computer systems is restricted to authorized people".

Based on point of impact of risks, controls are classified:

- Preventive controls: It prevent risks from actualizing.
- Detective controls: It detect the risks as they arise.
- Corrective controls: It facilitate correction.

### Sources of Risk

Most important step in risk management process is to identify sources of risk, the areas from where risks can occur. It gives information about possible threats, vulnerabilities & accordingly appropriate risk mitigation strategy can be adapted. Sources of risk includes:

- Commercial & Legal Relationships,
- Economic Circumstances,
- Human Behavior,
- Natural Events,
- Political Circumstances,
- Technology & Technical Issues,
- Management Activities & Controls, and
- Individual Activities.

### Risk Management Strategies

When risks are identified & analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor & it may not be cost effective to implement expensive control processes for them. Risk management strategy are:

- **Tolerate/Accept the risk**. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low.
- **Terminate/Eliminate the risk**. It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products & by seeking more capable suppliers & vendors.
- **Transfer/Share the risk**. Risk mitigation approaches can be shared with trading partners & suppliers. E.g. Outsourcing IT Infrastructure Management, Insurance, etc.
- **Treat/mitigate the risk**. Where other options have been eliminated, suitable controls must be devised & implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back**. Where probability or impact of risk is very low, then management may decide to ignore the risk.

### Key Governance Practices of Risk Management

- **Evaluate Risk Management:** *Continually examine the effect of risk on current & future use of IT* in the enterprise. Consider *whether the enterprise's risk appetite is appropriate & enterprise IT risks is within the risk appetite*;
- **Direct Risk Management:** *Direct the establishment of risk management to provide reasonable assurance that IT risk management practices are appropriate* to ensure that *Actual IT-risk does not exceed risk appetite*;
- **Monitor Risk Management:** *Monitor key goals & metrics of risk management processes* and *establish how deviations or problems will be identified, tracked & reported on for remediation*.

### Key Management Practices for Implementing Risk Management

- **Collect Data:** Identify & collect relevant data *to enable effective IT-related risk identification, analysis & 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 & risk attributes*, including expected frequency, potential impact, etc.
- **Articulate Risk:** Provide information on IT- related exposures & opportunities to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** *Manage opportunities & reduce risk to an acceptable level as a portfolio.*
- **Respond to Risk:** *Respond timely with effective measures to limit the magnitude of loss* from IT related events.

### Metrics of Risk Management

Enterprises have to monitor the processes & practices of IT risk management by using specific metrics. Some of key metrics are:

- Percentage of critical business processes, IT services & 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;
- Frequency of updating the risk profile based on status of assessment of risks.

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

## IT STRATEGY PLANNING

Planning is basically deciding in advance 'what is to be done', 'who is going to do' and 'when it is going to be done'. **There are 3 levels of managerial activity in an enterprise:**

- **Strategic Planning:** It is defined as the *process of deciding on 'objectives of the enterprise', 'on changes in these objectives', 'on resources used to attain these objectives', and 'on policies which govern the acquisition, use & disposition of these resources'. It is the process by which top management determines 'overall organizational purposes & objectives & how they are to be achieved.*
- **Management Control:** It is defined as the *process by which managers assure that resources are obtained & used effectively & efficiently in accomplishing of enterprise's objectives*.
- **Operational Control:** It is defined as the *process of assuring that specific tasks are carried out effectively & efficiently*.

IT strategic plans provide direction to deployment of IS & it is important that key functionaries in the enterprise are aware & are involved in its development & implementation.

### IT Strategic Planning Process

- It has to be *dynamic in nature.*
- *Ensure that a process is in place to modify & accommodate changes to enterprise's long-range plan & changes in IT conditions*.
- Establish a policy requiring that *IT long & short-range plan are developed & maintained.*
- *Ensure that IT long-range plan is regularly translated into IT short-range plans.* Such *short-range plans* should be *reassessed periodically & amended in response to changing business & IT conditions*.
- *Ensure adequate execution of short-range plans*.

### Objective of IT Strategy

- To provide a holistic view of the current IT environment,
- The future direction, &
- The initiatives required to migrate to the desired future environment.

### Classification of IT Strategy Planning

- **Enterprise Strategic Plan:** It provides overall charter under which all units in the enterprise, including Information Systems function must operate. It is primary plan prepared by top management guiding long run development.
- **IS Strategic Plan:** It focus on striking an optimum balance of IT opportunities & IT business requirements. It is done by forming long-term plans & translating them into short-term & operational plan.
- **IS Requirement Plan:** Every enterprise have to clearly define their IS Architecture, based on which IS Requirement Plan is drawn up to meet information requirement of the enterprise.
- **IS Application & Facilities Plan:** It is developed on the basis of IS Architecture & associated priorities. It includes specific application system to be developed & an associated time schedule; Hardware & Software acquisition/development schedule, etc.

### Key Management Practices for Aligning IT Strategy with Enterprise Strategy

- **Understand enterprise direction (i.e. enterprise objective):** Consider current enterprise environment & business processes, enterprise strategy & future objectives and external environment of the enterprise.
- **Assess the current environment, capabilities & performance (current IT):** Assess performance of current internal business & IT capabilities and external IT services, and develop an understanding of the enterprise IT architecture. Identify issues currently being experienced & develop recommendations for improvement.
- **Define the target IT capabilities:** Define the target business & IT capabilities & required IT services based on enterprise environment & requirements, assessment of the current business process & IT environment & issues and consideration of reference standards, best practices.
- **Conduct a gap analysis:** Identify the gaps b/w current & target environments. Consider the alignment of assets with business outcomes to optimize investment.
- **Define the strategic plan & road map (to close gap):** Create a strategic plan in co- operation with relevant stakeholders, which defines how IT-related goals will contribute to the enterprise's strategic goals. It include how IT will support IT business processes & initiatives to close gaps, etc.
- **Communicate the IT strategy & direction to stakeholders & users:** It create awareness & understanding of business & IT objectives & direction, as stated in IT strategy to stakeholders & users.

### Business Value from Use of IT

It is achieved by ensuring optimization of the value contribution to the business from business processes, IT services & IT assets resulting from IT-enabled investments at an acceptable cost.

**Key management practices for Implementing – Evaluation of 'Whether business value is derived from IT':**

- **Evaluate Value Optimization:** Continually *evaluate* the *portfolio of IT enabled investments, services & assets to determine the likelihood of achieving enterprise objectives & delivering value at a reasonable cost*. Identify if any changes is required to optimize value creation.
- **Direct Value Optimization:** *Direct value management principles & practices* to *enable optimal value realization from IT enabled investments throughout their economic life cycle*.
- **Monitor Value Optimization:** *Monitor key goals & metrics* to *determine the extent of business is generating expected value & benefits* to the enterprise *from IT-enabled investments & services*. *Identify significant issues & consider corrective actions.*

**The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments & services portfolio & how transparency of IT costs, benefits & risk is implemented.**

***Some key metrics for such evaluation:***

- Percentage of *IT enabled investments* where benefit realization monitored through full economic life cycle;
- Percentage of *IT services* where expected benefits have been realized;
- Percentage of *IT enabled investments* where claimed benefits met or exceeded;
- Percentage of *investment business cases* with clearly defined & approved expected IT related costs & benefits;
- Percentage of *IT services* with clearly defined & approved operational costs & expected benefits;
- *Satisfaction survey of key stakeholders* regarding transparency, understanding & accuracy of IT financial information.

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

**ROLE OF IT IN ENTERPRISES - (IT is key enabler & If IT fails then business fails too, that's why IT governance is importance)**

- In an increasingly digitized world, enterprises are using IT not merely for data processing but also for strategic & competitive advantage too.
- IT deployment has progressed from data processing to MIS to DSS to online transactions/services.
- IT has not only automated the business processes but also transformed the way business processes are performed.
- IT is used to perform business processes, activities & tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.
- The extent of technology deployment not only impacts the way internal controls are implemented in an enterprise but also provide better & innovative services from strategic perspective.
- Extensive organization restructuring or business process re-engineering may be facilitated through IT deployments.
- An IT strategy aligned with business strategy ensures value creation & facilitates benefit realization from the IT investments.

**COBIT (Control Objectives for Information and Related Technology)**

**COBIT** is a set of best practices for IT management developed by **Information Systems Audit & Control Association (ISACA)** and IT Governance Institute in 1996. ISACA develops & maintains the internationally recognized COBIT framework, helping IT professionals and enterprise leaders fulfill their IT Governance responsibilities while delivering value to business. **COBIT 5** is the only business framework for the governance & management of enterprise IT. This evolutionary version incorporates the latest thinking in enterprise governance & management techniques, and provides globally accepted principles, practices, analytical tools & models to help increase the trust in, and value from, IS.

| | | |
|---|---|---|
| **Need for Enterprises to Use COBIT 5**<br><br>**i.e. WHY COBIT** | Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance & management to address these critical business issues. COBIT 5 is useful for enterprises of all types & sizes, including non- profit & public sector and is designed to deliver business benefits to enterprises, including:----------→ | ○ *Increased value creation* from use of IT;<br>○ *User satisfaction* with IT engagement and services;<br>○ *Reduced IT related risks & compliance* with laws;<br>○ Development of more *business-focused IT solutions & services*;<br>○ Increased enterprise *wide involvement in IT-related activities*. |
| **Integrating COBIT 5 with Other Frameworks** | COBIT5 provides a basis to integrate effectively other frameworks, standards & practices used such as **ITIL, Val IT, ISO 27001, etc.** COBIT should be aligned with & in harmony with (amongst others) the:------→ | ○ Enterprise policies, strategies, governance, business plans, and audit approaches;<br>○ Enterprise risk management framework;<br>○ Existing enterprise governance organization, structures & processes. |
| **Components in COBIT** | • **Framework -** Organize IT governance objectives & good practices by IT domains & processes, and links them to business requirements;<br>• **Process Descriptions -** Process Reference Model & Common Language for everyone in an organization. The processes map to responsibility areas of plan, build, run & monitor.<br>• **Control Objectives -** Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.<br>• **Management Guidelines -** Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.<br>• **Maturity Models -** Assess maturity & capability per process & helps to address gaps. | |
| **Benefits of COBIT 5** | ○ It enables enterprises in *achieving their objectives for governance & management of enterprise IT*.<br>○ It helps enterprises to *create optimal value from IT* by maintaining a balance b/w realizing benefits & optimizing risk levels & resource use.<br>○ It *takes full end-to-end business & IT functional areas of responsibility considering the IT related interests* of internal & external stakeholders.<br>○ It helps enterprises to *manage IT related risk* and *ensures compliance, continuity, security & privacy*.<br>○ It enables clear *policy development & good practice for IT management* including increased business user satisfaction.<br>○ It is useful for enterprises of *all sizes, whether commercial, not-for-profit or in the public sector*.<br>○ It supports *compliance with relevant laws & regulations*. | |
| **Customizing COBIT 5 as per Requirement** | COBIT 5 can be tailored *(As per requirements of stakeholders)* to meet an enterprise's specific business model, technology environment, industry, location & corporate culture. Because of its open design, it can be applied to meet needs related to:<br>○ Information security, ○ Governance & management of enterprise IT, ○ Legislative & regulatory compliance,<br>○ Risk management, ○ Assurance activities, ○ Financial processing or CSR reporting.<br>Enterprises can select required guidance & best practices from specific publications & processes of COBIT 5. | |
| **COBIT 5 Process Reference Model** | COBIT 5 includes a Process Reference Model, which defines & describes in detail a number of governance & management processes of enterprise IT into 2 main process domains- **Governance** & **Management**.<br>It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT & business managers.<br>○ **Governance:** It involve ***evaluating*** stakeholder needs, conditions & options. Setting ***Direction*** through prioritization & decision making. ***Monitoring*** performance & compliance.<br>○ **Management:** It contains 4 domains, in line with the responsibility areas of ***Plan, Build, Run & Monitor*** **(PBRM)**. | |

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

| | |
|---|---|
| **Five Principle of COBIT 5** | • **Principle 1: Meeting Stakeholder Needs:** Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes & practices. Stakeholder needs have to be transformed into an enterprise's actionable strategy. *The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT related goals and enabler goals.* This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.<br>• **Principle 2: Covering Enterprise End-to-End:** *COBIT 5 integrates GEIT into enterprise governance. It covers all functions & processes within enterprise; COBIT 5 does not focus only on the 'IT function', but treats information & related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.* It considers all IT-related governance & management enablers to be enterprise-wide & end-to-end, i.e. inclusive of everything & everyone.<br>• **Principle 3: Applying a Single Integrated Framework:** There are many IT related standards & best practices, each providing guidance on a subset of IT activities. *COBIT 5 is a single & integrated framework as it aligns with other latest relevant standards & frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance & management framework integrator*.<br>• **Principle 4: Enable Holistic Approach:** Efficient & effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT *5 defines a set of enablers to support implementation of a comprehensive governance & management system for enterprise IT.* (Enablers are defined as anything that can help to achieve objectives of the enterprise.)<br>• **Principle 5: Separating Governance from Management:** *COBIT 5 framework makes a clear distinction b/w governance & management. These 2 disciplines encompass different types of activities, require different organizational structures & serve different purposes.* |
| **7 ENABLERS** Enablers are factors that individually or collectively influence whether governance & management will work over enterprise IT. | • **Principles, Policies & Frameworks** are vehicle to translate the desired behavior into practical guidance for day-to-day management.<br>• **Processes** describe an organized set of practices & activities to achieve certain objectives and produce outputs in support of overall IT-related goals.<br>• **Organizational structures** are the key decision-making entities in an enterprise.<br>• **Culture, Ethics & Behavior** of individuals & of enterprise is important but are underestimated as a success factor in governance & management activities.<br>• **Information** is pervasive throughout any organization & includes all information produced & used by the enterprise. Information is required for keeping the organization running & well governed.<br>• **Services, Infrastructure & Applications** include the infrastructure, technology & applications that provide the enterprise with IT processing & services.<br>• **People, Skills & Competencies** are linked to people & are required for successful completion of all activities & for making correct decisions & taking corrective actions. |
| **Risk Management in COBIT 5** | COBIT provides excellent guidance on risk management strategy & practices from governance & management practice.<br>The Governance domain contains 5 governance processes *to ensure that enterprise's risk appetite & tolerance are understood, articulated & communicated, and risk to enterprise value related to use of IT is identified & managed.* It also provides guidance on how to ensure that IT-related enterprise risk does not exceed risk appetite & risk tolerance. |

**IT COMPLIANCE REVIEW**

Failures of some large enterprises in last decade due to lack of adequate ERM has compelled regulators to mandate its enforcement thus necessitating compliance with **Governance, Risk and Compliance (GRC)**. As IT is a key enabler for most enterprises, it makes good sense to implement IT GRC as a sub-set of overall GRC under the regulatory umbrella of corporate governance.

**Sarbanes Oxley Act, Clause 49 of listing agreement issued by SEBI, Annexure as per CARO, Information Technology Act 2008 (provides legal recognition for electronic records & also mandates responsibilities for protecting information)** impose specific responsibilities on corporate. Hence, it can be said that implementing GRC is not only a management requirement but is mandated by law too.

**Compliance in COBIT 5**

- The management domain of "monitor, evaluate & assess" contains compliance focused process.
- This process is designed to evaluate that IT process & IT supported business process comply with laws, regulation & contractual requirements.
- This process ensures that enterprise comply with all applicable external requirement, enterprise governance-determined principles, policies & procedures.
- COBIT 5 also suggest accountability & responsibility for enterprise role & governance/management structure for each process.
- COBIT 5 also includes necessary guidance to support enterprise GRC objectives & supporting activities.
- COBIT combined with COSO has been the most widely used framework for implementing IT controls as part of enterprise risk management to meet governance requirements.

# CHAPTER – 1 CONCEPTS OF GOVERNANCE & MANAGEMENT OF INFORMATION SYSTEM

**Key Management Practices of IT Compliance (Provided by COBIT)**

- **Identify External Compliance Requirements:** Identify & monitor for changes in local & international laws, regulations & requirements that must be complied from an IT perspective.
- **Optimize Response to External Requirements:** Review & adjust policies, principles, standards, procedures & methodologies to ensure that legal, regulatory & contractual requirements and industry standards & codes of good practice are addressed & communicated.
- **Confirm External Compliance:** Confirm compliance of policies, principles, standards, procedures & methodologies with legal, regulatory & contractual requirements
- **Obtain Assurance of External Compliance:** Obtain & report assurance of compliance & adherence with policies, principles, standards, procedures & methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.

**Key Metrics for Assessing Compliance Process**

Sample metrics for reviewing the process of evaluating & assessing compliance with external laws & regulations and IT compliances with internal policies:

- **Compliance with External Laws & Regulations:**
  - Cost of IT related non-compliance, including settlements & fines;
  - Number of IT related non-compliance issues reported to the board or causing embarrassment;
  - Number of non-compliance issues relating to contractual agreements with IT service providers;
  - Coverage of compliance assessments.
- **IT Compliance with Internal Policies:**
  - Number of incidents related to non-compliance to policy;
  - Percentage of stakeholders who understand policies;
  - Percentage of policies supported by effective standards & working practices;
  - Frequency of policies review & updates.

**INFORMATION SYSTEM ASSURANCE**

In rapidly changing digital world, enterprises are inundated with new demands, strict regulations & risk scenarios emerging daily, making it critical to effectively govern & manage information & related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to stakeholders by ensuring effective use of IT.

**Using COBIT 5 for IS Assurance**

- Auditors will have to understand business processes, organization structure & enterprise's policies, procedures & practices.
- Enterprise executes its business operations through its staff who. These staff needs to have defined job responsibilities provided in organization structure.
- Organization structure needs to have internal control structure.
- COBIT 5 is designed to deliver benefits to both an enterprise's internal stakeholders (board, management, employees) & external stakeholders (customers, business partners, external auditors, shareholders, regulators)
- COBIT 5 is written in a non-technical language. Therefore, usable also by senior management personnel, assurance providers; regulators.
- COBIT can be used as an umbrella framework under which other standards & approaches (ITIL, ISO 27001) have been integrated into overall enterprise governance.

**Sample Areas of Review of Assessing & Managing Risks**

This review covers Controls over IT process of assessing & managing risks and is expected to provide assurance that the enterprise has identified enterprise IT Risk & mitigate these risks by appropriate cost effective risk management strategy.

Specific areas evaluated are:

- Risk management ownership & accountability
- Different kinds of IT risks (technology, security, continuity, regulatory)
- Defined & communicated risk tolerance profile
- Root cause analyses & risk mitigation measures
- Quantitative / qualitative risk measurement
- Risk assessment methodology
- Risk action plan & Timely reassessment.

**Evaluating & Assessing the System of Internal Controls**

COBIT 5 has specific process to **Monitor, Evaluate & Assess System of IC**", with objective to:

- Continuously monitor & evaluate control, including self-assessments & independent assurance reviews;
- Enable management to identify management deficiencies & inefficiencies to initiate improvement actions;
- Plan, organize & maintain standards for internal control assessment & assurance activities.

This review would provide assurance to stakeholders on adequacy of system of internal controls.

**Key management practices for assessing & evaluating the system of internal controls:**

- **Monitor Internal Controls:** Continuously monitor, benchmark & improve IT control to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls to ensure that controls within business processes operate effectively & maintain evidence for same.
- **Perform Control Self-assessments:** Encourage management & process owners to perform a continuing program of self - assessment to evaluate completeness & effectiveness of management's control over processes, policies & contracts.
- **Identify & Report Control Deficiencies:** Identify control deficiencies and analyze & identify their underlying root causes and report to stakeholders.
- **Ensure that assurance providers are independent & qualified:** Ensure that entities performing assurance are independent, have competence in skills & knowledge necessary to perform assurance and adherence to codes of ethics & professional standards.
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives & conformance objectives, assurance objectives, inherent risk, resource constraints & sufficient knowledge of enterprise.
- **Scope assurance initiatives:** Define & agree with management on the scope of assurance initiative, based on assurance objectives.
- **Execute assurance initiatives:** Execute planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, recommendations for improvement.

**Evaluating IT Governance Structure & Practices by Internal Auditors**

IT Governance can be evaluated by both external as well internal auditors. **The Institute of Internal Auditors (IIA)** has issued following guidance from internal audit perspective.

- **Leadership:** Following aspects need to be verified by auditor:
  - Relationship b/w IT objectives & strategic needs of the organization.
  - Involvement of IT leadership in development & on-going execution of organization's strategic goals.
  - Determine how IT will help organization to achieve these goals.
  - Review how roles & responsibilities are assigned within IT organization & how they are executed.
  - Review role of senior management & board in establishing & maintaining strong IT governance.
- **Organizational Structure:** Following aspects need to be assessed by auditor:
  - How organization management & IT personnel are interacting & communicating current & future needs across the organization.
  - Existence of necessary roles & reporting relationships to allow IT to meet the needs of organization.
- **Processes:** Following aspects need to be checked by auditor:
  - IT process activities & controls in place to mitigate risks & whether they provide reasonable assurance.
  - What processes are used by the IT organization to support consistent delivery of expected services?
- **Risks:** Following aspects need to be reviewed by auditor:
  - Processes used by the IT organization to identify, assess, & monitor/mitigate IT risks.
  - Determine accountability of personnel regarding risk management.
- **Controls:** Following aspects need to be verified by auditor:
  - Key controls defined by IT to manage its activities & support the overall organization.
  - Ownership, documentation & reporting of self-validation aspects.
  - Whether control are strong enough to address identified risks based on organization's risk appetite & tolerance levels, as well as any compliance requirements.
- **Performance Measurement/Monitoring:** Following aspects need to be verified by auditor:
  - Evaluate the framework & systems in place to measure & monitor organizational outcomes where support from IT plays an important role.

**Sample Areas of GRC (Governance, Risk & Compliance) for Review by Internal Auditors**

IIA provides areas, which can be reviewed by internal auditors as part of review of GRC areas:

- **Scope:** Internal auditor must evaluate & contribute to the improvement of governance, risk management & control processes using a systematic & disciplined approach.
- **Governance:** Internal auditor must assess & make recommendations for improving the governance process for:
  - Promoting ethics & values within organization;
  - Ensuring effective organizational performance management & accountability;
  - Communicating risk & control information to appropriate areas of organization;
  - Coordinating activities & communicating information among board, external & internal auditors, and management.
- **Evaluate Enterprise Ethics:** Internal auditor must evaluate design, implementation & effectiveness of organization's ethics related objectives, programs & activities. S/he should also assess whether IT governance supports organization's strategies & objectives.
- **Risk Management:** Internal auditor must evaluate the effectiveness & contribute to the improvement of risk management processes.
- **Interpretation:** Determining whether risk management processes are effective in a judgment resulting from internal auditor's assessment that:
  - Significant risks are identified & assessed;
  - Appropriate risk responses are selected that align risks with organization's risk appetite;
  - Relevant risk information is captured & communicated in a timely manner.
- **Risk Management Process:** Internal auditor may gather information to support this assessment during multiple engagements. It provide an understanding of organization's risk management processes & their effectiveness. Risk management processes are monitored through on-going management activities, separate evaluations, or both.
- **Evaluate Risk Exposures:** Internal auditor must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
  - Achievement of organization's strategic objectives;
  - Reliability & integrity of financial & operational information;
  - Effectiveness & efficiency of operations & programs;
  - Safeguarding of assets;
  - Compliance with laws, regulations, policies, procedures & contracts.
- **Evaluate Fraud & Fraud Risk:** Internal auditor must evaluate the potential for occurrence of fraud & how organization manages fraud risk.
- **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with engagement's objectives & be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained in risk management processes into their evaluation of organizations' risk management process. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by managing risks.

# CHAPTER – 2 INFORMATION SYSTEM CONCEPTS

**Information:**

- Processed data
- Data consists of facts, values or result and
  Information is result of relation b/w data. E.g.
  Data: Student name/roll no. /marks in science and arts.
  Information: Graph showing who acquired more than 80% in science & 65% in arts.
- Information may be represented in the form of text / graph / pictures /voices / videos etc.
- Information is data put into the meaningful & useful context. Mere collection of data is not information & mere collection of information is not knowledge.
- Information is essential because it adds knowledge, helps in decision making, analyzing future & acting in time.
- Information produced by IS can be represented by no. of ways.
  E.g. Paper reports, visual displays, multimedia displays, multimedia documents, electronic messages, graphics images & audio responses.

**Attributes/Characteristics of Information:**

1. **Availability:** Useless if not available in time of need.
2. **Purposes/Objective:** Must have some purpose/objective at the time of transmission, otherwise it is simple data. This helps in decision making, generating new concepts & ideas, identifying & solving problems, planning & controlling, etc.
3. **Modes & Format: Mode** may be in form of voice / text / combination of these two. **Format** should be simple, relevant & designed in such a way that is easily understandable by recipient & should assists in decision making, solving problems, initiating planning, controlling & searching.
4. **Current/Updated:** Refreshed form time to time as it usually rots with time & usage.
   E.g. running cricket score sheet & information about stock market.
5. **Rate:** Information should be transmitted at the rate which matches which rate at which recipient wants to receive it.
6. **Frequency:** Frequency with which information is transmitted or received affects its value.
   E.g. Weekly sales report is less reliable for assessing salesman capability as compared to quarterly reports.
7. **Completeness & Adequacy:** Information provided should be complete & adequate because only complete information can be used in policy making.
8. **Reliability:** Unreliable information leads to incorrect decision making.
9. **Validity:** How close information relates to purpose for which its serve.
   E.g. Experience of employee for evaluating their performances.
10. **Quality:** Means correctness of information.
    E.g. correct status of Profit/ Stock.
11. **Transparency:** Essential in decision & policy making.
12. **Value of Information:** Defined as difference b/w value of change in decision behavior caused by information & cost of information.

**System:** Defined as a group of interconnected components working towards accomplishment of a common goal by accepting inputs & producing outputs in an ordered transformation process.

**Systems Classification:**

| | |
|---|---|
| **Element Based Systems** | **Abstract System –** Also known as Conceptual System or Model that can be defined as an orderly arrangement of independent ideas or constructs.<br>E.g. System of theology about god & relationship of human with god. |
| | **Physical System –** Set of tangible elements, which operated together to accomplish an objective.<br>E.g. Computer System. |
| **Interactive Behavior Based System** | **Open System –** Interacts with other systems in its environment & change with changes in environment, survives in long term. |
| | **Closed System –** Not interact with environment & does not change with changes in environment, deteriorate over time. |
| **Degree Of Human Intervention Based** | **Manual System –** Activity like data collection, maintenance & final reporting done by human. |
| | **Automated System –** Activity like collection, maintenance & final reporting are carried out by computer system or say machine itself. |
| **Working/ Output Based** | **Deterministic System –** operates in predictable manner with certainty.<br>E.g. Math calculation by calculator. |
| | **Probabilistic System –** defined in terms of probable behaviour.<br>E.g. GPS, Whether Forecasting, Demand of goods. |

**Information System & Its Components:** with help of IS, enterprises & individuals can use computers to collect, store, process, analyze & distribute information.

- Manual Information System
- Computer Based Information System

| Components of Information Systems | | | | |
|---|---|---|---|---|
| **People**<br>-IT Professionals<br>-Administrator<br>-Programmer<br>-End user who uses IS for desired Info. | **Hardware**<br>Physical Components like<br>- server,<br>- terminals | **Software**<br>-System Software<br>-Application Software<br>-Utility Software | **Data**<br>Raw fact<br>Maybe in form of<br>-Database<br>-Text<br>-Image/Audio/Video | **Network**<br>Communication Media like<br>-Intranet<br>-Extranet<br>-Internet |

**Characteristics of CBIS** (Computer Based Information System)

1. Systems **work for predetermined objective** & is designed & developed accordingly.
2. System has number of **interrelated & independent subsystems or components**.
3. **No subsystems can function in isolation**, systems **depends on other subsystems for input**.
4. **Failure of one subsystem/component** may **bring down entire system**.
5. **Subsystems interacts with each other** to achieve the goal of system.
6. **Work done by individual subsystems is integrated to achieve the central goal of system**.
7. **Goal of Individual subsystem is of lower priority** than goal of entire system.

# CHAPTER – 2 INFORMATION SYSTEM CONCEPTS

| Major areas of computer based application | | | | |
|---|---|---|---|---|
| **Finance & accounting**<br>This subsystem ensures financial viability of org., enforce financial discipline, plan & monitor financial budget. It also helps in forecasting revenues, determining & managing financial resources in best possible way. It includes sub-application like –<br>✓ Financial accounting;<br>✓ General ledger;<br>✓ Accounts receivable/payable;<br>✓ Asset accounting;<br>✓ Investment management;<br>✓ Cash/Fund management;<br>✓ Balance sheet, etc. | **Marketing & sales**<br>This subsystem aims to maximize sales & ensure customer satisfaction. It facilitates order procurement by marketing / advertising products & creating new customers. Sales department uses order processing system to track orders, generate bills & delivering products, analyzing sales data in diff. region, computing commission to dealers / salesman, rendering services during warranty period & beyond. | **Production or manufacturing**<br>This subsystem aims to optimally deploy man, machine & material to maximize production or service. It generates schedules of production, material requirements, & monitors product quality, plans for replacement or overhauling of machinery & also helps in overhead cost control & waste control. | **Inventory/stores management**<br>This sub system keeps track to materials in stores. It regulate the maximum/minimum level of stocks, raise alarm at danger level stock, give timely alert for re-ordering of materials with optimal re-order quantity & facilitates stock management by solving various queries about inventory. | **Human resource management**<br>Human resource is most valuable asset for an org. This sub system aims to adequate utilization of manpower in most effective & efficient way through dispute-free environment to facilitate disruption free & timely services in business. Skill database (includes details of qualifications, training, experience, interests etc.) helps management to allocate manpower to right activity at time of need. It may include –<br>✓ Personnel administration;<br>✓ Recruitment management;<br>✓ Travel management;<br>✓ Benefit administration;<br>✓ Salary administration;<br>✓ Promotion management etc. |

| Types of Information System | | | |
|---|---|---|---|
| **Operational Level System (OSS)**<br>It support operational managers in tracking elementary activities like tracking customer order, invoice etc. It produces variety of information for internal & external use. Their role is to effectively process business transactions, control industrial processes, support enterprise communications & collaborations and update corporate database. Main objective of OSS is to improve operational efficiency of enterprise.<br>• TPS | **Knowledge Level System**<br>It supports discovery, processing & storage of knowledge & data. It supports business to integrate new knowledge into business & control paperwork & enable group working<br>E.g. Workstations.<br>• OAS<br>• KMS | **Management Level System**<br>It supports middle managers in monitoring, decision-making & administrative activities. It is helpful in answering questions like - are things working well & in order? It also ensures that business procedures are followed & provide periodic report rather than instant information.<br>• MIS<br>• DSS | **Strategic Level System**<br>SLS are for strategic managers to track & deal with strategic issues, assisting long-range planning. It support senior level management to tackle & address strategic issues and long term trends, both inside organization & outside world. It answers the questions like what products should be launched to increase profit & capture market.<br>• EIS |

**TPS (Transaction Processing System):**

- Developed for bottom / lowest level of management.
- It organize & manipulate data or transaction to generate various information for internal / external use.
- Process transactions like sales / purchase / delivery / payments etc. & demand data in detailed form. E.g. Tally / ATM / Admission software.

**Major activities of TPS**

- Capturing data to organize in files/database
- Processing files/databases using application software
- Generating information in form of reports
- Processing queries from various quarters of organizations.

**TPS Components:**

- **Input:** Source Documents (such as customer orders, slip & invoices employee time card) are physical inputs into TPS. They serve purposes like
  - Capturing Data
  - Indicating need to record data
  - Providing permanent file for future access & analysis if it is retained.
- **Processing:** After giving input, transaction gets processed & then only users gets an output. E.g. Journals, Register.
- **Storage:** It includes Ledger & Files which provide storage of data for future reference.
- **Output:** Any document generated in system is output. E.g. Financial Report summarizes the result of transaction processing & expresses it in accordance with principles of financial reporting. Some document are both input & output. E.g. Customer Invoice.

**Basic features of TPS:**

- **Large volume of Data:** As TPS is transaction oriented, it consist of large volume of data which require greater storage capacity. It ensures that data regarding economic activities are captured quickly & correctly.
- **Automation of basic operations:** TPS aims at automating basic operations & day-to-day functioning of business enterprise. Any failure in TPS can be havoc for enterprise.
- **Benefits are easily measurable:** It reduces workload of people associated with operations by automating some operations & improves their efficiency. Benefits of TPS are tangible & easily measurable. Thus it is easy to conduct cost benefits analysis & obtain user acceptance.
- **Source of input for other systems:** TPS is basic source of other Internal IS.

# CHAPTER – 2 INFORMATION SYSTEM CONCEPTS

**OAS (Office Automation System):** The application of computers to handle office activities is termed as office automation. It refers to integration of office functions related to managing information. Basic activities involved in OAS:

- **Document Capture:** Documents originating from outside sources like incoming mails, handouts etc. needs to be preserved.
- **Document Creation:** it consists of preparation of documents, dictation, editing etc. It takes major part of secretary's time.
- **Distributions:** It includes distribution of correspondence to designated recipients.
- **Filing, Search, Retrieval, Follow up:** It relates to filling, indexing, searching of documents which takes significant time.
- **Calculations:** It includes usual calculator functions like routine arithmetic, operations for bill passing, interest or % age calculations.
- **Recording utilization of resources:** It includes record keeping of utilization of specific resources by office personnel.

**Benefits of Office Automation Systems –**

- It improve communication within & b/w org.
- It reduces cycle time b/w preparation & receipt of messages.
- It also reduces costs of communication in terms of time & cost.
- It ensures accuracy of information & smooth communication flow.

## COMPUTER BASED OAS / TYPES OF OAS

**I. Text Processing Systems**

It is most commonly used components of OAS, as large proportion of office communication takes place in writing.
It automates process of development of documents such as letters, reports, memos etc. which reduce effort & minimizes chances of errors
It helps in quick production of multiple copies of document using printers, scanner etc.

**II. Electronic Document Management System**

It captures information contained in documents, store for future reference & make them available to users whenever required.
This is very useful in remote access of documents which is almost impossible with manual document management systems & in case of internal communication.
E.g. Loan application form filed in a branch can be accessed at head office or any office for scrutiny of loan proposals.

**IV. Teleconferencing & Video-conferencing Systems**

Teleconferencing is used in business meeting involving more than 2 persons located at 2 or more different places.
It reduces time & cost of meeting as participants do not have to travel to attend meeting.
It may be audio or video conferencing.

**III. Electronic Message Communication Systems –** Business enterprises uses variety of communication systems to send & receive messages for e.g. telephone, mail, Fax, etc. Computer based message communication systems reduces time & cost of sending or receiving messages and also enhance reliability of message.

**Components of Message Communication Systems**

1. **Electronic Mail**- Features of electronic mail:
   - ✓ **Electronic Transmission-** Transmission of email is electronic, hence very quick & almost instantaneous.
   - ✓ **Online Development & Editing -** Email message can be developed & edited online before transmission, which eliminates need of paper, & provide storage facility.
   - ✓ **Broadcasting & Rerouting** - Email permits rerouting & sending a message to large number of target recipients.
   - ✓ **Integration with other IS** - E-mail has advantage of being integrated with the other IS which helps in attaching attachments.
   - ✓ **Portability –** Email can be accessed from any Personal computer/tablet/smart phones.
   - ✓ **Economical -** Advancements in communication technology & competition among communication service providers have made Email most economical mode for sending & receiving messages.

**2. Facsimile (Fax) –** It is electronic communication of images of documents over telephone lines. It uses special software & fax servers to send & receive fax messages using common communication resources. Servers have ability to receive fax messages & automatically reroute them to the intended recipient after viewing it at central computer, similarly, a person can leave fax messages to server which will send it to the intended recipient automatically. Fax is gradually fading away with more use of emails.

**3. Voice Mail –** It is a variation of email in which messages are transmitted as digitized voice. Recipient can access e-mail box & hear messages in voice of sender. For security purpose it may require identification code before accessing voice mail.

**Knowledge Management System (KMS)** - The world is moving swiftly in direction of a knowledge-based system as enterprises adapt more & more cost-cutting measure. There is shift from an economy principally concerned by management of tangible resources (equipment, machinery, buildings, ....) to an economy in which renovation & growth are determined by intangible resources (knowledge, technology, competencies, abilities to innovate....). Information & Knowledge are key elements of this economy. A firm's competitiveness depends on its knowledge processing i.e. what it knows; how it uses & how fast it can know something new. It's much more influential than the harmony of land, labour & capital (i.e. three most important production factors).
Knowledge Management (KM) is process of capturing, developing, sharing, & effectively using organizational knowledge to achieve organizational objectives. KMS refers to any kind of IT system that stores & retrieves knowledge, improves collaboration, locates knowledge sources, mines repositories for hidden knowledge, captures & uses knowledge, & enhances KM process.

**Types of Knowledge:**

**Explicit knowledge:** It is formalized easily & easily available across org. in form of spoken words, written material & compiled data. This type of knowledge can be codified, easy to document, transfer & reproduce. E.g. online tutorials, Policy & procedural manuals.

**Tacit knowledge:** It resides only in few hands & is unarticulated & represented as intuition, perspective, beliefs & values that individuals form based on their experiences. It is difficult to document & communicate. E.g. hand-on skills, special know-how, employee experiences.

# CHAPTER – 2 INFORMATION SYSTEM CONCEPTS

**Management Information Systems (MIS) –** MIS enables management at different levels in decision making & problem solving by using results produced by TPS & other information. MIS is an integrated user-machine system designed for providing info. **to support operational control, management control & decision making functions** in an org.". **MIS is computer based system that provides flexible & speedy access to accurate data"**. It supports managers at different levels in decision making to achieve organizational goals. MIS at top level is comprehensive but is condensed / summarized at middle level management. It generates reports which can be displayed on demand or under exceptional conditions.

**Characteristics of an effective MIS:**

- **Management Oriented –** Development of IS should start from an appraisal of management needs & overall business objectives to meet requirement of top, middle or operating levels of management.
- **Management Directed –** Since MIS is management oriented, management should direct system's development by devoting sufficient time at designing, review & implementation stage of system development.
- **Integrated –** All sub- systems are tied together into one entity. An integrated IS has capability of generating more meaningful information to management as it takes comprehensive & complete view at org.
- **Common Data Flows –** It means use of common input, processing & output procedures whenever required. Data is captured only once which eliminates duplication in data collections, simplifies operations & make system more efficient.
- **Heavy Planning Element –** MIS development takes 1-3 years or even longer. Therefore, consider future information requirements & objectives as per organizational structure.
- **Sub System Concept –** MIS is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented in phased plan.
- **Common Database –** MIS is "super-file", which consolidates & integrates data stored in separate data files. Data can be accessed by several sub-systems which eliminates duplication in data storage, updating, deletion & protection.
- **Computerized -** Use of computers increases effectiveness, accuracy of system & consistency in processing data & reduce clerical staff.

**Pre-requisites of an Effective MIS –**

- **Database-** Data in database should be easily accessible with minimum redundancy. It should be
  - ✓ User-oriented.
  - ✓ Capable of being used as common data source to various users.
  - ✓ Available to authorized persons only.
  - ✓ Controlled by a separate authority.
- **Qualified System & Management Staff –**
  - ✓ Qualified system staff refers to computer experts who develop & maintains system & capable of understanding management concepts to facilitate understanding of problems faced by org.
  - ✓ Management staff refers to those who uses & understand operation of MIS & guide for types of information required.
- **Support of Top Management –** It is required for effectiveness of MIS in org.
  - ✓ If top management do not support MIS then it will also be not supported by subordinate & get lesser priority & may be delayed or abandoned.
  - ✓ To gain support of top management, officers should place before top management all supporting facts & state clearly the benefits accruing from it to org. to enlighten them.
- **Control & maintenance of MIS-** Some time, users develop their own procedures or short cut methods to use system, which reduce its effectiveness. Control ensures everyone operate system as it was designed to operate.
  It has to be improved with time, hence maintenance is required.
- **Evaluation of MIS –** MIS should meet information required by executives continuously. It can be achieved by evaluating MIS & taking appropriate action timely. It should consider:
  - ✓ Existence of flexibility in MIS to cope with expected or unexpected info. requirement in future.
  - ✓ Views of users & designers about capabilities & deficiencies of system.
  - ✓ Guiding appropriate authority to steps to maintain effectiveness of MIS.

**Constraints in operating a MIS –**

- **Non-availability of experts**, who can diagnose objectives of org. & provide direction to install suitable system & operate. We can overcome this problem by grooming internal staff by proper selection & training.
- **Experts face problem of selecting sub-system** of MIS to be installed & operated upon. We can overcome by understanding the criteria which guides need & importance of a function for which MIS can be installed first.
- Due to varied objectives of org., approach adopted by experts for designing & implementing **MIS is a non-standardized one**.
- **Non-availability of cooperation from staff** is a crucial problem, which should be handled tactfully by educating them by organizing lecturers, showing films to explain utility of system & involving them in development & implementation of system.

**Limitations of MIS –**

- Quality of outputs of MIS **depends on quality of input & processes**.
- MIS is not a substitute for management. It **cannot replace managerial judgment in making decisions**. It is merely a tool for executives for decision making & problem solving.
- MIS may **not quickly update itself** with change in needs with time.
- MIS is **not a tailor-made information packages suitable for every type of decision to be made** by executives.
- MIS takes **into account mainly quantitative factors & ignores non- quantitative factors** like morale & attitude of members of org., which is important for decision making.
- MIS is **less useful for making non-programmed decisions**. Such types of decisions are not routine type & thus require information, which may not be available in existing MIS.
- **Effectiveness** of MIS is **reduced** in enterprises having culture of **hoarding (not sharing) info**.
- **Effectiveness** of MIS **decreases due to frequent changes** in top management, organizational structure & operational team.

**Misconceptions about MIS –**

- Any computer based IS is a MIS.
- Any reporting system is MIS.
- It is a management technique.
- It is a bunch of technologies.
- It is a file structure.
- MIS is about use of computers.
- More data means more information to managers.
- Accuracy plays vital role in reporting.

# CHAPTER – 2 INFORMATION SYSTEM CONCEPTS

**Decision Support System (DSS) –** DSS is interactive software-based system intended to help decision making by compiling useful information from raw data, documents, personal knowledge, and/or business models to identify, solve problems & make decisions. It is defined as **system that provides tools to managers to assist them in solving semi-structured & unstructured problems**. It do not make decisions for managers, but rather generate information required by them in making decisions. DSS supports human decision-making process, rather than a means to replace it.

**Components of DSS –**

- **The user –** It include manager with unstructured/semi-structured problem to solve without having computer background.
  - ✓ **Manager -** They have basic computer knowledge & want DSS to be very user friendly, may be at any level either top or operating level.
  - ✓ **Staff Specialist (Analysts) -** They are more details oriented & are willing to use complex system in their day-to-day work.
- **Databases –** DSS includes routine & non-routine data from both internal (from TPS & MIS) & external (from EIS) sources.
  **Database is implemented at three levels:**
  - ✓ **Physical level –** It involves implementation of database on hard disk i.e. storage of data in hard disk.
  - ✓ **Logical Level –** It is designed by professional programs, which have complete knowledge of DBMS. It deals with nature of data stored, scheme of data. Storage is divided into various tables having rows & columns and techniques for defining relationships with indexes.
  - ✓ **External level –** Logical level defines schema, which is divided into smaller units known as sub-schemas which contain all relevant data needed by manager.
- **Model base –** It is "brain" of DSS because it performs data manipulations & computations with data provided to it by user & database.
- **Planning languages –**
  - ✓ **General-purpose planning languages** that allow users to perform many routine tasks like retrieval of data, statistical analyses. E.g. languages used in Excel spreadsheets.
  - ✓ **Special-purpose planning languages** are more limited in what they do, & they do certain jobs better than GPPL. E.g. programming language for PC.

**Characteristics of DSS**

- DSS **supports decision** making at all levels of management.
- It should also **help group** in making decisions instead of helping individuals only.
- It should be **flexible & adaptable** to change as per changes in environment.
- DSS focuses on **decision rather than data & information**.
- It should be **easy to use i.e. User Friendly.** User not having knowledge of computer programming should be able to generate reports with helps of DSS.
- It can be used for **structured problems**.
- It should be **extensible & evolve overtime.**
- DSS are used for **decision making rather than communicating decisions**.

**Examples of DSS in Accounting –**

- **Cost Accounting System -** Health care industry is well known for its cost complexity. Managing costs in such industry require controlling costs of supplies, expensive machinery, technology, & variety of personnel. Cost accounting applications help health care enterprises to calculate product costs for individual procedures or services. DSS can accumulate these product costs to calculate total cost per patient.
- **Capital Budgeting System –** Decision makers need to supplement analytical techniques (like NPV or IRR) with decision support tools. DSS allows decision makers to consider financial, non-financial, quantitative, & qualitative factors in their decision-making processes. Using DSS can evaluate multiple investment alternatives at once.
- **Budget Variance Analysis System –** Financial institutions rely heavily on their budgeting systems for controlling costs & evaluating managerial performance. DSS generate variance reports & allow them to analyze variances in tabular & graphical form to forecast budget.
- **General Decision Support System –** DSS also solves general accounting problems like ratio analysis, working capital or debtor management etc.

**Executive Information Systems (EIS) –** Also referred to as Executive Support System (ESS). It serves strategic level i.e. top level managers. It **creates generalized computing & communications environment rather than providing any preset applications or specific competence**.

**Characteristics of EIS –**

- EIS is Computer-based-information system that **serves info. need of top executives**.
- EIS enables users to **extract summary data** without need to learn query languages, statistical formulas or high computing skills.
- EIS provides **rapid access to timely information**.
- EIS is capable of accessing both **internal & external data**.
- EIS provides **extensive online analysis tool** like trend analysis, market conditions analysis, etc.
- EIS can be given as **DSS support for decision making**.

**The Executive Decision-Making Environment –** Executives make decisions based on vision to make their enterprise successful. They rely mostly on their own intuition. The intuitive character of decision-making reflects types of information useful to executives.

**Characteristics of information used in EIS**:

- **Lack of structure –** Decisions made by executives are relatively unstructured & not as clear-cut. It is not always known, 'which data are required' or 'how to weigh available data in decision making.'
- **High degree of uncertainty –** Results of decision are not scientifically predictable & are often characterized by lack of precedent.
- **Future orientation –** It is executive's responsibility to make sure that org. keeps pointed toward future & take strategic decisions to shape future events. They need to take care about future

**Contents of EIS –** EIS includes "whatever is interesting to executives"
**A practical set of principles** to guide the design of measures and indicators to be included in an EIS:

- EIS measures must be easy to understand & collect data. Data should be collected naturally as part of process of work.
- EIS measures should not add substantially to workload of managers/staff.
- EIS measures must be based on balanced view of organization's objective in areas of productivity, resource management, and quality & customer service.
- Performance indicators in EIS must reflect everyone's contribution in fair & consistent manner.

technologies, competition & future government policies.

- **Informal Source –** Executives rely heavily on informal source for key information. E.g. lunch with a colleague in another firm, information form TV might reveal some important competitor strategies.
- **Low level of detail –** Executive decisions are made by observing broad trends which requires awareness of large overview than tiny items i.e. sometimes, answers to some questions found by going through details.

- EIS measures must encourage management & staff to share ownership of organization's objectives.
- EIS information must be available to everyone in organization to provide them information about organization's performance.
- Confidential information should not be part of EIS of organization.
- EIS measures must evolve to meet changing needs of organization.

**DIFFERENCE BETWEEN DSS & TRADITIONAL MIS**

| | DSS | Traditional MIS |
|---|---|---|
| **Philosophy** | Provide integrated tools, data, models & languages to end users | Provide structured info. to end users |
| **Orientation** | External orientation | Internal orientation |
| **Flexibility** | Highly flexible | Relatively inflexible |
| **Analytical capability** | More analytical | Little analytical |
| **System analysis** | Emphasis on tools to be used in decision process | Emphasis on info. requirement analysis |
| **System design** | Interactive process | System development based on static info. requirements |

**DIFFERENCE BETWEEN EIS & TRADITIONAL INFORMATION SYSTEMS**

| | EIS | Traditional IS |
|---|---|---|
| **Nature of Information Access** | Specific issues/problems & aggregate reporting | Status reporting |
| **Level of management** | Top Executives | Lower staff |
| **Nature of info. provided** | Online tools analysis | Offline status reporting |
| **Drill down facility** | Available | Not available |
| **Information Sources** | More external, less internal | Internal |
| **Information format** | Text with graphics | Tabular |
| **Nature of interface** | User-friendly | Computer-operator generated |

**Expert System -** ES is highly developed DSS that utilizes knowledge generally possessed by an expert to solve a problem. ES imitate reasoning processes of human experts & provide decision makers with expert type advice. ES have ability to explain reasoning process that was used to make decisions.
E.g. ES of investment portfolio management might ask about specific questions like – how much can be invested / preferences regarding any securities, etc.

**Business applications of Expert Systems**:

- **Accounting & Finance -** It provides tax advice & assistance, investment advice, helping with credit- authorization decisions.
- **Marketing -** It establish sales quotas, respond to customer inquiries, determining discount policies.
- **Manufacturing -** It determine whether a process is running correctly by analyzing quality & providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting product design, etc.
- **Personnel -** It helps in assessing applicant qualifications & assist employees in filling forms.
- **General Business -** It helps to assist project proposals, recommending acquisition strategies, educating trainees & evaluating performance.

**Properties of Expert System:**

- **Availability –** Experts must be capable of communicating problems to which ES will be applied.
- **Complexity –** ES should be able to solve complex task which requires logical inference processing.
- **Domain –** The domain, or subject area of problem is relatively small & limited to a relatively well-defined problem area.
- **Expertise –** Solutions to problem requires effort of experts. Only few possess knowledge, techniques, & intuition needed.
- **Structure –** Solution process must be able to cope with ill-structured, uncertain, missing, & conflicting data.

**Benefits of Expert Systems –**

- ES preserve knowledge that might be lost through retirement / resignation / death of expert.
- ES put information into an active-form so it can be said almost as a real-life expert.
- ES assist novices in thinking in way experienced professional do.
- ES are not emotional.
- ES can be used as strategic tool in areas of marketing & improving products, cutting costs.

**Need for Expert Systems –**

- Expert labor is **expensive & scarce**. Hence, companies cannot easily find & keep experts.
- Expert can only handle few factors at a time, but **ES can handle all factors at a time.**
- Due **practical limit on quality of human decision making** put a need for ES.

**ERP** - It is process management software that allows org. to use integrated applications to manage business & automate many back office functions related to technology, services & human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales & marketing. It requires dedicated teams to customize & analyze data & to handle upgrades & deployment.

**ERP Packages**
ERP System is multi-module software system. It integrates all business process & functions of entire Enterprise into single software system using single integrated database shared across org., which automates business activities of functional area within org. E.g. a module designed to process purchasing transactions which record all data about purchase orders & integrated with accounts payable & inventory records.

# CHAPTER – 2 INFORMATION SYSTEM CONCEPTS

**Components of ERP:** ERP model is consists of **4 components**

- **Software Component:** It is most visible part & consists of several modules such as Finance, HR, SCM, SRM, CRM, & Business Intelligent.
- **Process Flow:** It is model that illustrates the way how info. flows among different modules within ERP system to understand how ERP work.
- **Customer mindset:** By implementing ERP system, old ways of working which user understand & comfortable with have to be changed which may lead to users' resistance. E.g. some users may say that they have spent many years doing excellence job without help from ERP system. Company have to eliminate negative value or belief so that users may accept new system.
- **Change Management:** During ERP implementation, change needs to be managed. E.g. User resistance to change & Business process changes.

**Benefits of ERP**

- Streamlining processes & workflows with single integrated system.
- Reduce redundant data entry & processes & shares information across org.
- Establish uniform processes based on recognized best business practices.
- Improved workflow & efficiency.
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- Reduced inventory costs resulting from better planning, tracking & forecasting of requirements.
- Turn collections faster based on better visibility into accounts & fewer delivery errors.
- Decrease in vendor pricing by taking better advantage of quantity breaks.
- Track actual costs of activities & perform activity based costing.
- Provide a consolidated picture of sales, inventory & receivables.

**Core Banking System (CBS)** - It is banking services provided by group of networked bank branches where customers may access their bank A/c & perform basic transactions from any branch offices. Banks make these services available across multiple channels like ATMs, Internet banking & branches, etc.
CBS may be defined as back-end system which processes daily banking transactions & posts updates to accounts & other financial records. E.g. deposit, loan & credit-processing.

**Elements of core banking**:

- Making & servicing loans, opening new accounts.
- Processing cash deposits & withdrawals.
- Processing payments & cheques.
- Calculating interest, establishing interest rates.
- Customer Relationship Management (CRM).
- Managing customer accounts.
- Establishing criteria for minimum balances, interest rates, number of withdrawals allowed, etc.
- Maintaining records for all bank's transactions.

**Various types of Business Applications**

IS has changed traditional business system by providing everything on just a mouse click, at anytime, anywhere. IT improved communication by online meeting & instant exchange of information, irrespective of their location. IS provides innovative ideas to managers to keep competitive edge.

1. **Accounting Information System (AIS)**: It comprises of processes, procedures & system that capture accounting data from business process, record it & process it to give summarized & consolidated report for external & internal use. Earlier accounting systems were paper based manual records & now enterprises uses computers to maintain such records.

   **Key steps of AIS**:

   - Work steps within business process to capture accounting data.
   - Manual / Computer based records to record accounting data.
   - Work steps for internal control.
   - Work steps to process, classify & consolidate raw accounting data.
   - Work steps that generate both internal & external reports.

2. **The impact of IT on IS for different sectors:**

- **E-business –** It includes purchasing, selling, production management, logistics, communication, support services & inventory management through use of internet technologies. It involves use of computers, routers, communication media etc. It's advantage are 24 hour sale, lower cost due to no rent of physical structure, eliminate middlemen, unlimited market with broaden customer base because of no limitation of time & space, secure payment systems, easier business administration. Only investment is needed for purchase of space on internet, designing & maintenance of website. E.g. B2B, B2C, C2C & C2B.
- **Financial Service Sector –** It includes banks, insurance companies, etc. They manages large amounts of data & processes enormous numbers of transactions every day. IT has changed working style of this sector by providing financial services on internet, accessible from anywhere & anytime. It reduces their cost & improve customer relationship.
  E.g. now money can be deposited or withdrawn form ATM instead of going to bank, payment can be made through internet banking, etc.
- **Wholesaling & Retailing –** Retail business uses IT for selling items, capturing sales data, stock control, buying, reporting, customer information & accounting. E.g. laser scanners used in most big bazars to read product bar codes. IT can be used in wholesale for logistics management, space management, purchasing, re-ordering, & analysis of promotions. Data mining & data warehousing helps in analysis of sales trends, customer profile etc.
- **Public sectors –** Hospitals, police stations, universities etc. uses IT/IS to keep records. E.g. IS like ERP used in university to keep record of its employees (designation, leaves availed, department, achievements) that can be used further in analyzing their performance, filing FIR without going to police station personally & important documents like passports can be made by online application.
- **Others –** IT is also used in entertainment industry (games, picture collection etc.), agriculture industry, Tour industry (railway, hotel & airline reservations) & consultancy etc.
- IT has changed the working style of business world drastically & made it simple through its advancement.

# CHAPTER – 2 INFORMATION SYSTEM CONCEPTS

Business uses IT for selling, capturing sales data, stock control, buying, reporting, customer information, decision making, accounting etc. **IT tools crucial for business growth.**

- **Business Website –** Website makes business reachable to large no. of customers. It can also be used in cost effective advertisement & CRM. Websites can be designed by using HTML, XML etc.
- **Internet & Intranet –**Time & space is no more obstacles for conducting meeting of people from multiple locations because of Internet. Intranet permits electronic exchange of data within an org., E-commerce provides new platform for conducting business in faster & easier way & also provides B2B, B2C, C2C, C2B communication with a click of mouse.
- **Software & Packages –** DBMS, data warehousing, data mining tools, knowledge discovery can be used for getting information that plays important role in decision making. E.g. by having information of buying habits of customer with use of data mining tools - marketing strategy can be built quickly & effectively.
- **Business Intelligence** (BI) – It **collect, provide access, analyze & store data & information about companies operations**. It is also used to analyze performance or internal operations e.g. EIS, CRM, business planning / finance / budgeting / marketing tools. E.g. Data mining, data warehouses, DSS etc.
- **Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc. -** Webcam, microphone etc. are used in conducting long distance meeting. It increases accuracy, reduce processing times, enable quick decisions & speed up customer service. E.g. Scanner in Big bazar.

**To operate IS effectively & efficiently, a business manager should have following knowledge about it:**

- **Foundation Concepts –** It includes fundamental business & managerial concepts e.g. 'what are components of system & their functions', or 'what competitive strategies are required'.
- **Information Technologies (IT) –** It includes operation, development & management of hardware, software, data, networks, & other technologies.
- **Business Applications –** It includes major uses of IT in business steps i.e. processes, operations, decision making, & strategic/competitive advantage.
- **Development Processes –** It comprise how end users & IS specialists develop & execute business / IT solutions to problems.
- **Management Challenges –** It includes 'how the function & IT resources are maintained & utilized to attain top performance & build business strategies'.

**Implications of IS in business:**

- IS helps managers in efficient decision-making to achieve organizational goals.
- Organization will be able to survive & thrive in highly competitive environment on strength of well-designed IS.
- IS helps in making right decision at right time.
- Good IS may help in generating innovative ideas for solving critical problems.
- Knowledge gathered though IS may be utilized by managers in unusual situations.
- IS is viewed as a process, it can be integrated to formulate strategy of action or operation.

**Information as a Key Business Asset & its Relation to Business Objectives & Processes**

Information is strategic resource which helps enterprises in achieving long term objectives & goals. In today's competitive & unpredictable business environment, only those enterprises survive, which have complete information & knowledge of customer buying habits & market strategy. Information management enhances organization's ability & capacity to deal with & achieve its mission by meeting challenges of competition, timely performance & change management.

**Role of Information in Business**

In today's dynamic business environment, it becomes mandatory to have complete information & knowledge of customer buying habits & market strategy for any enterprise. Timeliness, accurate, meaningful & action oriented information enhances an organization ability & capacity to deal with & develop in mission, competition, performance & change.

**Categorization of information:**

- **Top Level Management:** It comprise of owners/shareholders, Directors, KMP, etc. & are involved in decision & policy making. They require strategic information that helps them in making strategy. E.g. customers buying habits helps them to decide the launching of new products.
- **Middle Level Management:** It comprise of heads of functions departments & divisional sectional officers. They require tactical information that helps in implementing decisions taken by top management. Tactical information is used for short term planning whereas strategy information is used for long term planning. E.g. information of customers likely to purchase certain product can help sales managers to fulfill their sales target efficiently.
- **Lower Level Management:** It comprise of superintendents, supervisor, etc. They require operational information for smooth running of day-to-day activities like stock on hand, customer order pending etc. E.g. if a regular customer demands for product other than daily purchase then this information is important for salesman to deliver better service.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

## NEED FOR PROTECTION OF IS

**Organizations depend on timely, accurate, complete, valid, consistent, relevant, & reliable information**. Executive management has responsibility to ensure that organization provides all users with secure information processing environment.

There are direct & indirect benefits from using IS as well as risk. These risks have led to a gap b/w need to protect systems & degree of protection applied. The gap caused by:

- **Widespread use** of technology;
- **Interconnectivity** of systems;
- **Elimination of distance, time, & space** as constraints;
- Unevenness of **technological changes**;
- **Delegation** of management & control;
- Unconventional **electronic attacks**; and
- **Regulatory** requirements or technological developments

Information security failures may result in both financial losses and/or intangible losses. E.g. unauthorized disclosure of competitive or sensitive information.

## IS SECURITY

- Information security refers to **protection of valuable assets** from threats, sabotage or natural disaster **with physical safeguards** (locks, perimeter fences & insurance) or **logical & other technical safeguards** (user identifiers, passwords, firewalls).
- **Valuable assets are data / information recorded, processed, stored, shared, transmitted, or retrieved** from an electronic medium.
- The data / information is protected against harm from **threats** that **will lead to its loss, inaccessibility, alteration, or wrongful disclosure**.
- That **protection is achieved through layered series of technological & non-technological safeguards** like physical security & logical measures.

**IS Security Objective:**

- **Protection of interests of those relying on information.**
- **Protect IS & communications that deliver information from harm resulting into failures of CIA.**

**What Information is Sensitive?**

**Strategic Plans:** Most organizations acknowledge that strategic plans are crucial to success of company but they fail to protect these plans. E.g. competitor learns that company is testing new product line in specific geographic location.

**Business Operations:** Business operations consist of organization's process & procedures, it may provide market advantage to organization. E.g. when one company can provide service at lower price than competitor, then company's client lists & prices charged for various products & services can also be damaging.

**Finances:** Financial information (e.g. salaries & wages) are very sensitive & should not be made public. E.g. Availability of information about product pricing may be used by competitive enterprises to price its products competitively.

## INFORMATION SECURITY POLICY

- It is **statement of intent by management** about how to protect company's information assets.
- It is **formal statement of rules**, which give access to people to organization's technology & information assets.
- It is **document describing organization's information security controls & activities**.
- It does not specify technologies or specific solutions; it **defines specific set of intentions & conditions** that helps to protect company's information assets & its ability to conduct business.
- It is essential **foundation for effective & comprehensive information security program**. Information security concerns are translated into specific measurable & testable goals & objectives, and provides guidance to install & maintain IS.
- It intends to:
  - **Preserve & protect** information from **unauthorized modification / access / disclosure**;
  - **Limit / eliminate potential legal liability**; and
  - **Prevent waste / inappropriate use of resources** of org.
- It should be in **written** form providing instructions to employees
  - 'what kinds of behavior or resource usage are required & acceptable', &
  - 'what is unacceptable'.

**Tools to Implement Policy:**

- **Standards** – specify technologies & methodologies to be used to secure systems.
- **Guidelines** – assist user / system personnel / others, ensures security measures not overlooked & helps in smooth implementation of information security policy.
- **Procedures** – Detailed steps to accomplish a particular security related tasks.

These should be promulgated throughout an organization through handbooks or manuals.

**Issues to address**

Information Security policy addresses many issues (like CIA), **who may access what information & in what manner, basis on which access decision is made, separation of duties, who controls & who owns information, authority issues**.

This policy should clearly state senior management's commitment to information security & signed by appropriate authority & at least address following:

- **definition** of information security,
- **reasons** why information security is **important**, and its **goals & principles**,
- **brief explanation** of security policies, principles, standards & compliance requirements,
- definition of information security **responsibilities**; &
- reference to supporting **documentation**.

Auditor should ensure that policy is accessible to employees & employees are aware of its existence & understand its contents, and has owner who is responsible for its maintenance.

**Members of Security Policy (3 Groups of management)**

- **Management members** who have budget & policy authority.
- **Technical group** who know what can & cannot be supported.
- **Legal experts** who know legal consequences of various policy charges.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**Information Security Policies & their Hierarchy**

**Information Security Policy –** It provides definition of Information Security, its objective & importance that applies to all users.

**Types of information security policies**:

- **User Security Policies**
  - **User Security Policy –** It specifies responsibilities & requirements for all IT system users. It provides meaning of security for Users, Line Managers & System Owners.
  - **Acceptable Usage Policy –** It specifies policy for use of email, Internet services & other IT resources.
- **Organization Security Policies**
  - **Organizational Information Security Policy –** It sets out policy for security of its information assets & IT systems processing such information.
  - **Network & System Security Policy –** It sets out policy for system & network security for IT department users.
  - **Information Classification Policy –** It sets out policy for classification of information.
- **Conditions of Connection –** It sets out policy for connecting to the network for all organizations connecting to the Group.

**Components of Security Policy:** Good security policy should clearly state:

- **Purpose & Scope** of Document & intended **audience**;
- **Security Infrastructure**;
- Security policy **document maintenance & compliance requirements**;
- **Incident response & reporting mechanism**;
- Security **organization Structure**;
- **Inventory & Classification of assets**;
- Description of **technologies & computing structure**;
- **Physical & Environmental Security;**
- **Identity Management & access control**;
- **IT Operations management;**
- **IT Communications;**
- **System Development & Maintenance Controls;**
- **Business Continuity Planning;**
- **Legal Compliances;**
- **Monitoring & Auditing** Requirements.

## INFORMATION SYSTEMS CONTROLS

Increasing use of IT in organizations has made it imperative that appropriate IS are implemented. IT should cover all key aspects of business processes & should have an impact on its strategic & competitive advantage for its success. **IS controls ensures that business objectives are achieved & undesired risk events are prevented, detected & corrected.**

**Need for Controls in Information Systems**

Enterprises need **information integrity, reliability & validity** for timely flow of accurate information throughout the organization **to reduce probability of data loss, computer abuse, incorrect decision making & to maintain privacy**. Organization's management must set up system of IC, safeguard assets to maintain CIA of data.

IS should have controls for all sensitive or critical sections. IS control procedure may include:

- Access to IT resources, data & programs;
- System development methodologies & change control;
- Operation procedures;
- Physical Access Controls;
- BCP & DRP;
- Network & Communication Control;
- Database Administration;
- Protective & detective mechanisms against attacks etc.

**Objectives of Controls**

**Control** is defined as **Policies, procedures, practices & enterprise structure** that are designed to provide reasonable assurance that **business objectives will be achieved & undesired events are prevented, detected & corrected**. IS Auditing includes review of implemented system, providing consultation & evaluating reliability of operational effectiveness of controls.

**Objective of controls** is to **reduce or eliminate causes of exposure** to potential loss. All exposures have **causes** such as:

- Errors/omissions in data, procedure, processing;
- Improper authorizations & improper accountability; &
- Inefficient processes / procedures.

**Control objectives serve two main purposes:**

- Outline policies of org. laid down by management; &
- Provide benchmark for evaluating whether control objectives met.

*(Exposures – Potential losses due to threats materializing)*

**Some of critical control lacking in computerized environment:**

- Lack of management understanding of IS risks & related controls;
- Absence / inadequate IS control;
- Lack of awareness & knowledge of IS risks & controls;
- Complexity of implementation of controls in distributed computing environments;
- Lack of control features or their implementation in highly technology driven environments;
- Inappropriate technology or inadequate security implementations.

**Impact of Technology on Internal Controls**

- **Competent & Trustworthy Personnel:** Personnel should have proper skill & knowledge to discharge their duties.
- **Segregation of Duties:** Processing of transaction is split b/w different people so that one person cannot process a transaction right from start to finish. It prevents or detects errors or irregularities. In computerized system, auditor should concerned with segregation of duties within IT department.
- **Authorization Procedures:** In manual system, auditor evaluate adequacy of procedures for authorization. In computer systems, authorization procedures often are embedded within a computer program. E.g. programmed credit limit approvals.
- **Adequate Documents & Records:** In computer systems, documents might not be used to support initiation, execution, & recording of some transactions. Thus, no visible audit trail would be available to trace transactions. Hence, controls over protection & storage of documents, transaction details, & audit trails etc. should be placed properly.
- **Physical Control over Assets & Records:** It is critical in both manual systems & computer systems. In manual systems, it is done through use of locked doors & filing cabinets. Computerised systems have not changed the need to protect data. Client's data & computer programs can be maintained at single site i.e. computer location, and it has increased the threat of computer abuse or disaster due concentration of information at one place.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

- **Adequate Management Supervision:** In manual system, management supervision is relatively easy as managers & employees are often at same physical location. In computer system, data communication facilities can be used to enable employees to be closer to customers they service. Thus supervision of employees might have to be carried out remotely. The Management's supervision and review helps to deter and detect both errors & fraud.
- **Independent Checks on Performance:** In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures. If program code in computer system is authorized, accurate, & complete, then system will always follow designated procedures in absence of other failure like hardware or software failure.
- **Comparing Recorded Accountability with Assets:** Data & assets should periodically compared to determine incompleteness / inaccuracies in data or shortages / excesses occurred in assets. In manual system, independent staff prepares basic data to be used for comparison. In computer system, software is used to prepare such data.
- **Delegation of Authority & Responsibility:** A clear line of authority & responsibility is an essential control in both manual & computer systems. In computer system, delegating authority & responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

## CLASSIFICATION OF INFORMATION SYSTEMS CONTROLS

**CLASSIFICATION ON THE BASIS OF "OBJECTIVE OF CONTROLS"**

### 1. Preventive Controls:

Preventive Controls are those, which are designed to prevent an error, omission or malicious act from occurring. E.g. use of passwords.

**Characteristics of preventive controls:**

- Clear understanding about vulnerabilities of asset;
- Understanding probable threats; and
- Provision of necessary controls for probable threats from materializing.

Control can be implemented in both manual & computerized environment for same purpose, implementation methodology may differ from one environment to other.

**Examples of preventive controls (for both manual & computerized)**

- Employing qualified personnel;
- Segregation of duties;
- Access control;
- Vaccination against diseases;
- Documentation;
- Training of staff;
- Authorization of transaction;
- Validation, edit checks in application;
- Firewalls;
- Anti-virus software etc.

| Purpose | Manual Control | Computerized Control |
|---|---|---|
| Restrict unauthorized entry into premises | Build gate & post security guard | Use access control software, smart card, biometrics, etc. |
| Restricted unauthorized entry into software applications | Keep computer in secured location & allow only authorized person to use applications | Use access control, viz. User ID, password, smart card, etc. |

### 2. Detective Controls:

These controls are designed to detect errors, omissions or malicious acts that occur & report their occurrence.
E.g. Automatic expenditure profiling.

**Characteristics of detective controls:**

- Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.;
- An established mechanism to refer such reported unlawful activities to appropriate person or group;
- Interaction with preventive control;
- Surprise checks by supervisor.

**Examples of detective controls**

- Hash totals;
- Checking of calculations;
- Periodic performance reporting with variances;
- Past-due accounts report;
- Internal audit functions;
- Cash counts & bank reconciliation & monitoring expenditures against budgeted amount.

### 3. Corrective Controls:

Corrective controls are designed to reduce impact or correct an error once it has been detected.
E.g. use of default dates on invoices. BCP is considered as corrective control.

**Characteristics of corrective controls:**

- Minimize impact of threat;
- Identify cause of problem;
- Providing Remedy to problems discovered by detective controls;
- Getting feedback from preventive & detective control.
- Correcting error arising from problem;
- Modify processing systems to minimize future occurrences of incidents.

**Examples of corrective controls**

- Contingency planning;
- Backup procedure;
- Rerun procedures;
- Change input value to information system.

### 4. Compensatory Controls:

Controls are basically designed to reduce probability of threats, which can exploit vulnerabilities & cause loss to asset.

While designing control one thing should be kept in mind - **"The cost of lock should not be more than cost of assets it protects."**

There should be adequate compensatory measures, which may not be appropriate control, but reduces probability of loss to the assets. Such measures are called compensatory controls.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**CLASSIFICATION ON THE BASIS OF "NATURE OF INFORMATION SYSTEM RESOURCES**

**1. Environmental Controls:** These are controls relating to IT environment such as power, AC, UPS, smoke detection, fire- extinguishers, etc. It deals with external factors in IS & preventive measures to overcome these conflicts.

**Controls for Environmental Exposures**

**Fire Damage**
- Both automatic & manual fire alarms.
- Master switches for power & automatic fire suppression system.
- Fireproof Walls, Floors & Ceilings surrounding Computer Room & use Fire Resistant Office Materials.
- Fire exits, Fire Alarms, Fire Extinguishers, Fire Brigade Nos., Smoke detectors, etc.
- Less use of Wood & plastic in computer rooms.
- Regular Inspection by Fire Department.
- Wiring Placed in fire resistant Electrical Panels & Conduit.

**Power Spikes** (Caused due to very short pulse of energy in power line)
- **Power Failure:** Use UPS/Generator.
- **Power Supply Variation:** Use Voltage regulators & circuit breakers.
- **Emergency Power-Off Switch for emergency evacuation**.

**Water Damage** (water pipes burst, cyclones, tornadoes, floods)
- **Water Detectors:** Placed under raised floor, near drain holes.
- **Locating Computer Room at top floors.**
- Waterproofing, Adequate drainage system, Water leakage Alarms, etc.

**Pollution & Other Damages** (E.g. Dust on surfaces of magnetic tape / disk may cause damage to data)
- Prohibit Eating, Drinking & Smoking within Information Processing Facility with clear sign on entry door.
- Clean dust, use AC.

**2. Physical Access Controls:** These are controls relating to physical security of tangible IS resources & intangible resources stored on tangible media. E.g. Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged, CCTV monitoring. It should be designed in such a way that it allows access only to authorized persons.

**Physical Access Issues & Exposures**
- Abuse of data processing resources
- Blackmail
- Embezzlement;
- Damage or theft of equipment or documents
- Disclosure of sensitive information
- Unauthorized entry.

**Possible perpetrators:** Employees, who are:
- Outrageously violates rules;
- Addicted to substance / gambling;
- Having financial / emotional problems;
- Former employee;
- Part time & Interested / informed outsiders (competitors, thieves, hackers)
- To be terminated;
- On strike;
- Threatened by disciplinary action / dismissal.

**Facilities that need to be protected:**
- Communication channels
- Dedicated telephone lines/cables
- Computer room
- LAN, server
- Switches, Router
- Storage devices & media
- Power & Backup sources
- Input/output devices
- Control units & front-end processors
- Microcomputer & PC

**Controls for Physical Access Exposures**

**Locks on Doors*:**
- **Cipher locks (Combination Door Locks)** - used in low security situations or where large number of entrances & exits are required. Door will unlock by entering 4 digit number for predetermined period of time (e.g. 10-30 seconds).
- **Bolting Door Locks** – Special metal key is required to gain access in case bolting door lock. To avoid illegal entry, the keys should not be duplicated.
- **Electronic Door Locks** – Magnetic or embedded chip-based plastics card (smart card) or token may be entered into a reader to gain access.

**Physical Identification Medium:**
- **Personal Identification numbers (PIN):** A secret number assigned to individual, in conjunction with some means of identifying the individual, to identify & authenticate such individual. Visitor will be asked to insert card & enter PIN to authenticate.
- **Plastic Cards** used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.
- **Identification Badges-** Identity cards issued to personnel as well as visitors. For easy identification purposes, its colour can be different.

**Logging on Facilities:**
- **Manual Logging:** All visitors should be prompted to sign visitor's log indicating their name, purpose of visit, time etc. A valid ID e.g. driver's license, business card, etc. may be asked before allowing entry.
- **Electronic Logging:** It is combination of electronic & biometric security systems. Users logging can be monitored & unsuccessful attempts being highlighted.

**Other means of Controlling Physical Access:**
- **Video Cameras** at specific locations & monitored by security guards.
- **Security Guards** aided with CCTV.
- **Controlled Visitor Access:** A responsible employee should escort all visitors.
- **Bonded Personnel:** All service contract personnel (E.g. cleaning staff) should be asked to sign bond. It do not improve physical security but limit financial exposure.
- **Dead Man Doors:** It contains pair of doors & second door opens once first door is locked. First door can open only by authorised user. Space b/w doors allow only one person to enter to prevent piggybacking.
- **Non–exposure (i.e. no explicit indication) of Sensitive Facilities.**
- **Computer Terminal Locks:** It ensure that devices to desk is not turned on by unauthorized persons.
- **Controlled Single Entry Point** monitored by receptionist. Multiple entry points increase chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.
- **Alarm System** to avoid illegal entry.
- **Perimeter Fencing** at boundary.
- **Employees who are out of office** for longer duration during office hours should be monitored carefully.
- **Secured Report/Document Distribution Cart** e.g. mail, post box must be covered & locked and should always be attended.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

***Advantages of electronic door locks over bolting & combinational locks:**

- Through Special Internal Code, cards can be made to identity correct individual.
- Individuals access needs can be restricted through internal code & sensor devices. Restrictions can be imposed to particular doors/hours/time.
- Degree of duplication is reduced.
- Card can be easily deactivated in case an employee is terminated or card is lost / stolen.
- If unauthorized entry is attempted, silent or audible alarms can be automatically activated.
- An administrative process dealing with Issuing, accounting for & retrieving card keys, are also parts of security.
- Biometric Door Locks: It is extremely secure since it uses individual's unique body features, e.g. voice, retina, fingerprint or signature, etc. Generally used in extreme sensitive case e.g. military.

**3. Logical Access Controls:**

These are controls relating to logical access to information resources. It is implemented to ensure that access to systems, data & programs is restricted to authorized users to safeguard information against unauthorized use, disclosure or modification, damage or loss.

Logical access controls are **system-based mechanisms used to designate access right of system resources and type of transactions & functions that are permitted**.

- Logical access controls restrict users to authorized transactions & functions.
- Exercise logical controls over network access.
- Controls implemented to protect integrity of application & confidence of public when public access the system.

**(i) Logical Access Paths**

**Online Terminals -** To access an online terminal, user has to provide valid login-ID & password. If additional authentication mechanisms are added along with password, it will strengthen security.

**Operator Console –** It is place where any intruders can play havoc. Hence, access to operator console must be restricted by:

- Keeping operator console at a place visible all.
- Keeping operator console in protected room accessible to selected personnel.

**Dial-up Ports:** Using a dial up port, user at one location can connect remotely to another computer present at an unknown location via telecommunication media. **Modem** is device which can convert digital data transmitted to analog data (one that telecommunication device uses). Thus, modem can act as interface b/w remote terminal & telephone line. Security is achieved by identifying remote users to determine authorisation to access.

**Telecommunication Network:** In Telecommunication network, number of computer terminals, PC etc. are linked to host computer through network or telecommunication lines, which could be private or public, security is provided to each route in same manner as in online terminals.

**(ii) Logical Access Issues and Exposures**

Controls that reduce the risk of misuse, theft, alteration or destruction should be used to protect unauthorized & unnecessary access to computer files. E.g. Restricting & monitoring computer operator activities in batch-processing environment. The opportunities of access in online system is more, hence level of control for this system must be more complex.

Access control mechanisms should applied not only to computer operator but also to end users, security administrator, management, and any other authorized users. It provide security to:

- Application Software
- System Software
- Telecommunication Lines
- Password library
- Data
- Data dictionary/directory
- Logging files
- Backup files

**Access Control Mechanisms:** It processes the users request in **3 Step**

- **Identification:** First users have to identify themselves.
- **Authentication:** Secondly, users must authenticate themselves. The mechanism accesses previously stored information about users, resources they can access, and action privileges they have w.r.t. such resources; then it permits or denies the request.
- **Authorization:** Third, users request for specific resources, their need & areas of usage of those resources. 2 approaches to implement authorization module in access control mechanism:
  - **Ticket-oriented approach** - Access control mechanism assigns users, a ticket for each resource they are permitted to access. Its primary advantage is its **run-time efficiency**. A **capability list** can be **stored in some fast memory device**. When user seeks access to a resource, access control mechanism simply looks up the capability list to determine whether such user is permitted to take desired action or not.
  - **List-oriented approach** - Mechanism associates with each resource a list of users who can access & action privileges that each user has w.r.t. such resource. Its advantage is that it **allows efficient administration of capabilities**. **Capabilities for a resource** can be controlled since they are **stored in one place**. One can examine access control list just to know who has access over the resource & can revoke or delete access to a resource.

**(iii) Issues and Revelations related to Logical Access *(Exposures to Logical Issue)***

Compromise or absence of logical access controls may result in potential losses due to exposures that may lead to total shutdown of the computer functions. Intentional or accidental exposures of logical access control encourage technical exposures & computer crimes.

**Technical Exposures:**

It includes unauthorized implementation or modification of data & software.

**Computer Crime Exposures:**

Computers can be utilized both constructively & destructively. Computer systems are used to steal

**Asynchronous Attacks:**

It occur in environments where data can be moved asynchronously across telecommunication lines. Numerous

**Remote & distributed data processing applications can be controlled in many ways.**

- Remote access to computer &

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**1. Data Diddling:** It involves the change of data before or after they are entered into system. A limited technical knowledge is required to data diddle & worst part is that it occurs before computer security can protect the data.

**2. Bomb:** It is piece of bad code deliberately planted by insider or supplier of program.

- **Logical Bomb:** An event triggers a bomb.
- **Time Bomb:** Triggers on time basis.

Bombs explode when conditions of explosion get fulfilled & causes damage immediately. However, these programs cannot infect other programs, since it do not circulate by infecting other programs.

**3. Trojan Horse:** It is malicious programs that are hidden under any authorized program. It is illicit coding contained in legitimate program, and causes illegitimate action. Trojan is similar to bombs but computer clock or particular circumstances do not necessarily activate it. Trojan may:

- Change or steal password or
- Modify records in protected files or
- Allow illicit users to use systems.

Trojan Horses hide in host & generally do not damage host program. Trojans cannot copy themselves to other software in the same or other systems. Trojan may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies Trojan program.

E.g. Christmas Card was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw Christmas tree & send copies of similar output to all other users connected to network because of which other users cannot save their unfinished work.

**4. Worm:** A worm does not require a host program like Trojan to relocate itself. Worm program copies itself to another machine on network. Since, worms are stand-alone programs, & they can be detected easily in comparison to Trojans & computer viruses. E.g. Alarm Clock worm places wake-up calls on list of users.

**5. Rounding Down:** It is rounding off small fractions of denomination & transferring these small fractions into perpetrator account. As amount is small, it gets rarely noticed.

**6. Salami Techniques:** It is slicing of small amounts of money from computerized transaction or account. It is slightly different from rounding technique, the fix amount is deducted. E.g. in rounding off technique, ` 23,456.39 becomes ` 23,456.40, while in Salami technique ` 23,456.39 is truncated to either ` 23,456.30 or ` 23,456.00.

**7. Trap Doors:** It allow insertion of specific logic or unauthorized logic.

E.g. program that interrupts review of data.

money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made. It can damage reputation, morale & even existence of organization. Computer crimes generally result in Loss of customers, embarrassment to management & legal actions against org.

**1. Financial Loss:** It may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

**2. Legal Repercussions:** Org. has to adhere many laws while developing security policies & procedures. These laws protect both perpetrator & organization from trial. Org. will be exposed to lawsuits from investors & insurers if there have no proper security measures.

**3. Loss of Credibility or Competitive Edge:** To maintain competitive edge, companies (e.g. bank) need credibility & public trust. Credibility will be shattered if security violation occurs, and will result in loss of business & prestige.

**4. Blackmail/Industrial Espionage:** By knowing confidential information, perpetrator can obtain money from organization by threatening & exploiting security violation.

**5. Disclosure of Confidential, Sensitive or Embarrassing Info.:** It can spoil reputation of organization, & may result in Legal or regulatory actions against company.

**6. Sabotage:** People not interested in financial gain but want to spoil credibility of company. They do it because of their dislike towards org. or for their intemperance.

**7. Spoofing:** Spoofing attack involves forging one's source address. One machine is used to impersonate other in spoofing technique. A penetrator makes the user think that s/he is interacting with OS.

E.g. Penetrator duplicates login procedure & captures user's password, attempts for system crash & makes user login again.

transmissions must wait for clearance of line before data being transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks;

**1. Data Leakage:** Data is critical resource for org. to function effectively. It involves leaking information out of computer by means of dumping files to paper or stealing computer reports & tape.

**2. Subversive Threats:** Intruder attempts to violate integrity of some components in sub-system. Subversive attacks can provide intruders with important information about messages being transmitted & intruder can manipulate such messages in many ways. By using:

- **Invasive tap:** By installing it on communication line, s/he may read & modify data.
- **Inductive tap:** It monitors electromagnetic transmissions & allows data to be read only.

**3. Wire-tapping:** It involves spying on information being transmitted over telecommunication network.

**4. Piggybacking:** It is act of following authorized person through secured door or electronically attaching to authorized telecommunication link that intercepts & alters transmissions. It involves intercepting communication b/w OS & user and modifying them or substituting with new messages.

**5. Shutting Down of Computer / Denial of Service:** It is initiated through terminals or microcomputers that are directly or indirectly connected to computer. It is known as Connection Flooding. When overloading happens, some systems shut down themselves. Hackers use this technique to shut down computer systems over Internet. (E.g. Flooding receiver's server with illegitimate request which prevent legitimate request from access)

data files through network should be implemented.

- Having terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems & other devices should be controlled appropriately.
- Terminal & computer operations at remote locations should be monitored carefully & frequently for violations.
- To prevent unauthorized access to system, there should be proper control mechanisms over system documentation & manuals.
- Data transmission over remote locations should be controlled. Sender should attach needed control information that helps receivers to verify genuineness & integrity.
- When replicated copies of files exist at multiple locations, ensure that all identical copies contain same information & checks are also done to ensure that duplicate data does not exist.

**Logical Access Violators**

They are often same people who exploit physical exposures, although skills needed to exploit logical exposures are more technical & complex. They are mainly:

**1. Hackers**: Hackers try their best to overcome restrictions to prove their ability.

**2. Employees** (authorized or unauthorized);

**3. IS Personnel**: They have access to computerized information. Segregation of duties & supervision help to reduce logical access violations;

**4. Former Employees** who left organization on unfavorable terms;

**5. End Users**; Interested Outsiders, Competitors; Organized Criminals; Crackers, etc.

**(iv) Logical Access Control across System**

Logical access controls serve as one of means of information security. The purpose of logical access controls is to restrict access to information assets/resources. Access should not be so restrictive that it makes performance of business functions difficult or it should not be so liberal that it can be misused i.e. it should be just sufficient for one to perform one's duty without any problem or restraint.

| | |
|---|---|
| **User Access Management** | **User Registration-** Information about every user is documented. The de-registration process is equally important.<br>**Privilege management-** Access privileges are to be aligned with job requirements & responsibilities.<br>**User password management-** Allocations, storage, revocation & reissue of password are password management functions.<br>**Review of user access rights-** User access right changes with time & requires periodic review.(E.g. Change in Job profile lead to change in access right) |
| **User Responsibilities** | **Password use-** Use of strong passwords to maintain confidentiality.<br>**Unattended user equipment-** Users should ensure that none of equipment under their responsibility is ever left unprotected. |
| **Network Access Control**<br>Internet connection exposes an org. to entire world. Hence, benefits should derive along with the precaution against harmful elements. | **Policy on use of network services-** Policy applicable to internet service requirements aligned with business need. (E.g. Policy-Selection of Appropriate services)<br>**Enforced path-** It is necessary to specify exact path or route connecting networks; E.g. internet access by employees will be routed through firewall & proxy.<br>**Segregation of networks** based on sensitive information handling function. E.g. VPN connection b/w branch & head-office, isolated network from internet services.<br>**Network connection & routing control-** Traffic b/w networks should be restricted based on identification of source & authentication access policies.<br>**Security of network services-** Techniques of authentication & authorization policy should be implemented across organization's network.<br>**Firewall-** Organizations connected to Internet & Intranet often implements electronic firewall to protect their network from intrude. All traffic b/w external network & organization's Intranet must pass through firewall. Only authorized traffic is allowed to pass through firewall.<br>**Encryption-** Encryption is conversion of data into secret code for storage in databases & transmission over networks. Sender uses encryption algorithm & original message called clear text is converted into cipher text (using private key). This is decrypted at receiving end (using public key).<br>**Call Back Devices-** The call- back device requires user to enter password & then system breaks connection. If caller is authorized, call back device dials caller's number to establish new connection.<br>**Recording of Transaction Log:** Intruder may penetrate system by trying different passwords & user ID combinations. All incoming & outgoing requests along with attempted access should be recorded in transaction log. E.g. user ID, time & terminal location from where request for access has been originated. |
| **OS Access Control**<br>*OS not only provides platform for application to use various IS resources & perform specific business function but is also the last barrier to be conquered for unlimited access to all resources. Hence, protecting OS access is extremely crucial.* | **Automated terminal identification-** It ensure that a particular session could only be initiated from a particular location or computer terminal.<br>**Terminal log-in procedures-** The log-in procedure does not provide unnecessary help or information, which could be misused by an intruder.<br>**Access Token-** If log on attempt is successful, OS creates an access token that contains key information about user like user-id, password & privileges granted etc. The access token is used to approve all actions attempted by user during session.<br>**Access Control List-** It is list containing information about access privileges for all valid users. When user attempts to access a resource, system grant access after verifying user-id & privileges contained in access token with access privileges contained in Access Control List.<br>**Discretionary Access Control-** Access to specific resources may be granted to specific users. E.g. Granting read only privilege for general ledger to budgeting department and granting read & write permission to A/Cs payable manager.<br>**User identification & authentication-** Users must be identified & authenticated. Biometric Authentication or Cryptographic means (DSC) may be employed.<br>**Password management system-** OS could enforce selection of good passwords. Password file should be accessible to user.<br>**Use of system utilities-** System utilities are programs that help to manage critical functions of OS. This utility should be strictly controlled & be not accessible to general user. E.g. addition/deletion of users.<br>**Duress alarm to safeguard users-** If users are forced to execute some instruction under threat, system provide a means to alert authorities.<br>**Terminal time out-** Log out the user if terminal is inactive for defined period, which prevent misuse in absence of authorized user.<br>**Limitation of connection time-** Predetermined available time slot. E.g. no computer access after 8.00 p.m. & before 8.00 a.m. - or on Saturday or Sunday. |
| **Application & Monitoring System Access Control** | **Information access restriction-** A user is allowed to access only to authorized items. Controls are implemented on the access rights of users, E.g. read, write, delete, & execute. Ensure that sensitive output is sent only to authorized terminals & locations.<br>**Sensitive system isolation-** Sometimes, it may even be necessary to run the system in an isolated environment.<br>**Event logging-** Maintain extensive logs for all types of events. Review whether logging is enabled & logs are archived properly. An intruder may penetrate system by trying different passwords & user ID combinations. All incoming & outgoing requests along with attempted access should be recorded in transaction log.<br>**Monitor system use-** Based on risk assessment, constant monitoring of some critical systems is essential. The extent of detail & frequency of review would be based on criticality of operation & risk factors. The log files are to be reviewed periodically & attention should be given to any gaps in these logs.<br>**Clock synchronization-** Event logs maintained across an enterprise network plays a significant role in correlating an event & generating report on it. Hence, need for synchronizing clock time across the network as per a standard time is mandatory. |
| **Mobile Computing** | Now computing facility is not restricted to a particular data centre alone. Ease of access on move provides efficiency & results in additional responsibility on management to maintain information security.<br>Theft of data carried on disk drives of portable computers (laptop) is high risk factor. Both physical & logical access is critical. Information is to be encrypted & access identifications like fingerprint, eye-iris, & smart cards are necessary security features. |

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

## CLASSIFICATION ON THE BASIS OF "AUDIT FUNCTIONS"

**Managerial Controls:** It ensure development, implementation, operation & maintenance of IS in planned & controlled manner in org. The controls at this level provide stable infrastructure in which IS can be built, operated, & maintained on day-to-day basis.

**Top Management & Information Systems Management Controls**

**Top Management**
Top management must ensure that IS function is well managed.
They are primarily responsible for long-run policy decisions on how IS will be used in org.

Controls adapted by management are to ensure that IS function correctly & meet strategic business objectives. They have responsibility to determine whether the control put in place are sufficient to ensure that IT activities are adequately controlled. **They are responsible for preparing a master plan for IS function.**

i. **Planning –** This includes determining goals of IS function & means of achieving such goals.
   - **Preparing the plan:**
     - **Recognizing opportunities & problems where IT & IS can be applied cost effectively;**
     - **Identify resources needed to provide required IT & IS; and**
     - **Formulating strategies & tactics for acquiring such needed resources.**
   - **Types of Plans:** Top management must prepare (& review & update regularly as the need arise)
     - **Strategic Plan: It is long-run plan covering, say, next 3 to 5 years of operations;**
     - **Operational Plan: It is short-plan covering, say, next 1 to 3 years of operations.**
   - **Role of a Steering Committee:** SC shall comprise of representatives from all areas of business & IT personnel. **The ultimate responsibility for IS planning should be vested to IS steering committee. They should assume overall responsibility for activities of IS function.**

ii. **Organizing –** This includes gathering, allocating, & coordinating resources needed to accomplish goals that are established during Planning Function.
   - **Resourcing IS Function:** Acquire resources needed to accomplish goals & objectives set out. E.g. hardware, software, personnel, finances, etc.
   - **Staffing IS Function: Acquisition, Development & Termination of IS personnel.**

iii. **Leading –** This includes motivating, guiding & communicating with IS personnel **to achieve harmony of objectives; i.e. a person's / group's objectives must not conflict with objectives of org.** (There is no best way of motivating & guiding and Effective communication promote good relationship & trust)

iv. **Controlling –** This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.

**Systems Development Management**
They are responsible for analyzing, designing, building, implementation & maintaining IS.

System Development Controls ensures that proper documentations & authorizations are available for each phase of system development process.
Activities dealing with system development controls in IT setup:

- **System Authorization Activities:** To ensure economic justification & feasibility, each new system request be submitted in written form by users to systems professionals who have both expertise & authority to evaluate & approve (or reject) request
- **User Specification Activities:** Users must be actively involved in systems development process & should create written detailed description of his needs.
- **Technical Design Activities:** It translate user specifications into set of detailed technical specifications of system that meets user's needs.
- **Internal Auditor's Participation:** Auditor should involve at inception of SDLC process to make suggestions regarding system requirements & controls. Auditor's involvement should be continued throughout all phases.
- **Program Testing:** All program modules must be tested before implementation. Then results are compared against predetermined results to identify errors.
- **User Test & Acceptance Procedures:** Just before implementation, individual modules of system must be tested as a unified whole. A test team comprising user personnel, systems professionals, & internal audit personnel. Once test team is satisfied that system meets its stated requirements, system is formally accepted by user department(s).

**Programming Management**
They are responsible for programming new system; maintain old systems & providing general systems support software.
Program development life cycle comprises six major phases:

| | |
|---|---|
| **Planning** | Techniques like PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan. |
| **Control**<br>It has 2 major purposes: | • **Task progress in various software life-cycle phases should be monitored against plan & corrective action should be taken in case of any deviations.**<br>• **Control over software development, acquisition, & implantation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.** |
| **Design** | A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted. |
| **Coding** | Programmers must choose a **module implementation & integration strategy** (Top-down, Bottom-up & Threads approach), a **coding strategy** (that follows percepts of structured programming), & a **documentation strategy** (to ensure program code is easily readable & understandable). |
| **Testing**<br>3 types of testing can be undertaken: | • **Unit Testing** – which focuses on individual program modules;<br>• **Integration Testing** – Which focuses in groups of program modules; and<br>• **Whole-of-Program Testing** – which focuses on whole program.<br>These tests are to ensure that a developed or acquired program achieves its specified requirements. |
| **Operation & Maintenance**<br>3 types of maintenance : | Management establishes formal mechanisms to monitor status of operational programs so maintenance needs can be identified on timely basis.<br>• **Repair Maintenance** – in which program errors are corrected;<br>• **Adaptive Maintenance** – in which the program is modified to meet changing user requirements; and<br>• **Perfective Maintenance** - in which the program is tuned to decrease the resource consumption. |

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**Data Administration**
They are responsible for addressing planning & control issues in relation to use of an organization's data.

**Data Resource Management Controls**

Data is critical resource that must be managed properly. Hence, centralized planning & control are implemented. For data to be managed; Users must be able to share data; data must be available when it is needed, in the location where it is needed, & in the form in which it is needed. Further it must be possible to modify data & integrity of data be preserved. Data must be controlled carefully because consequences are serious if the data definition is compromised / destroyed. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining & monitoring logs of data administrator's & database administrator's activities.

The control activities involved in maintaining integrity of the database is as under:

***(a)*** **Definition Controls: It ensure that the database always corresponds & comply with its definition standards.**

***(b)*** **Existence/Backup Controls: It ensure the existence of database by establishing backup & recovery procedures.** Backup refers to making copies of the data to restore the original data after a data loss. It ensures availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster. Various backup strategies:

- **Dual recording of data**: 2 complete copies of database are maintained & are concurrently updated.
- **Periodic dumping of data**: Periodic dump of all / part of database onto some backup storage medium. E.g. magnetic tape, removable disk, Optical disk
- **Logging input transactions**: Logging input data transactions which cause changes to the database
- **Logging changes to the data**: Copying a record each time it is changed by an update action.

***(c)*** **Access Controls:** It prevent unauthorized individual from **viewing, retrieving, computing or destroying** entity's data. It is established in following manner:

- **User Access Controls:** Through passwords, tokens & biometric Controls; and
- **Data Encryption:** Keeping data in database in encrypted form.

***(d)*** **Update Controls:** It restrict update of database to the authorized users in 2 ways:

- By permitting **only addition of data** to the database; and
- Allowing users to **change or delete existing data**.

***(e)*** **Concurrency Controls:** It provide solution to overcome data integrity problem which arise when 2 update processes access same data item at same time.

***(f)*** **Quality Controls:** It ensure the **accuracy, completeness, & consistency of data** maintained in the database. This may include traditional measures such as **program validation of input data** and **batch controls over data in transit** through the organization.

**Quality Assurance Management**
They are responsible for ensuring IS development, implementation, operation, & maintenance conform to established quality standards.

**Quality Assurance Management Controls**

**QA Management ensures that–**

- IS produced by IS function achieve certain quality goals; and
- Development, implementation, operation & maintenance of IS comply with a set of quality standards.

**Reasons for Emergence of QA in many organizations:**

- Organizations are increasingly **producing safety-critical systems** & users are becoming more demanding in terms of **quality of software** they employ to undertake their work.
- Organizations are undertaking more **ambitious projects** when they build software.
- Users are becoming more demanding in terms of their **expectations about the quality of software** they employ to undertake their work,
- Organizations are becoming more **concerned about their liabilities** if they produce & sell defective software.
- **Poor quality control** over the production, implementation, operation, & maintenance of software can be costly in terms of missed deadlines, dissatisfied users & customer, lower morale among IS staff, higher maintenance and strategic projects that must be abandoned.
- Improving the quality of IS is a part of a worldwide trend among organizations to **improve the quality of goods & services they sell**.

**QA Personnel should work to improve the quality of IS produced, implemented, operated, and maintained in an organization. They perform a monitoring role for management to ensure that –**

- Quality goals are established & understood clearly by all stakeholders; and
- Compliance with the standards to attain Quality IS.

**Security Administration**
They are responsible for access controls & physical security over IS function.

**Security Management Controls**

Information security administrators are responsible for ensuring that IS assets (**categorized under Personnel, Hardware, Facilities, Documentation, Data, Application Software, & System Software)** are secure. Assets are secure when expected losses that will occur over some time, are at an acceptable level.

Threat Identification: Threat is some action / event that can lead to a loss. During threat-identification phase, security administrators attempt to flesh out all material threats that can result in IS assets being exposed, removed (temporarily / permanently), lost, damaged, destroyed or used for unauthorized purposes.

Major Security threats and their control measures

| Threat | Controls |
|---|---|
| **Fire** | Well-designed, reliable fire-protection systems must be implemented. |
| **Water** | Facilities must be designed & sited to mitigate losses from water damage. |

Control's classification on basis of "Nature of IS Resources – Environmental Controls, Physical Controls & Logical Access Controls (*discussed earlier)* are all security measures against possible threats.

| | |
|---|---|
| **Energy Variations** | Voltage regulators, Circuit breakers & Uninterruptable power supplies can be used. |
| **Structural Damage** | Facilities like BCP, DRP, & Insurance etc. to withstand structural damages that may occur due to earthquake, snow, wind, etc. |
| **Pollution** | Regular cleaning of facilities & equipment. |
| **Unauthorized Intrusion** | Physical access controls can be used. |
| **Viruses & Worms** | Controls to prevent use of virus-infected programs & to close security loopholes that allow worms to propagate. |
| **Misuse of software, data & services** | Code of conduct to govern the actions of IS employees. |
| **Hackers** | Strong, logical access controls to mitigate losses from the activities of hackers. |

However, in spite of the controls on place, there could be a possibility that a control might fail. When disaster strikes, it still must be possible to recover operations & mitigate losses USING THE LAST RESORT CONTROLS - **DRP and Insurance.**

- **DRP: DRP comprise 4 parts – Emergency Plan, Backup Plan, Recovery Plan, & Test Plan. It lays down policies, guidelines, & procedures for all IS personnel.** BCP Controls are related to having an operational & tested IT continuity plan, which is in line with the overall business continuity plan & its related business requirements, so as to make sure that IT services are available as required & ensure minimum impact on business in the event of major disruption.
- **Insurance**: Adequate insurance must be able to replace IS assets & cover extra costs associated with restoring normal operations. Policies usually can be obtained to cover the resources like – Equipment, Facilities, Storage Media, Valuable Papers and Records etc.

**Operations Management** They are responsible for planning & controlling day-to-day operations of IS. (i.e. daily running of hardware and software facilities).

**Operations Management Controls** (Operations management typically performs controls over the functions as mentioned below)

***(a)*** Computer Operations: The controls over computer operations govern the activities that directly support day-to-day execution of either test or production systems on the hardware/software platform available. 3 types of controls fall under this category:
- **Operation controls**: It prescribe the functions that either human operators or automated operations facilities must perform.
- **Scheduling controls**: It prescribe how jobs are to be scheduled on a hardware/software platform.
- **Maintenance controls**: It prescribe how hardware is to be maintained in good operating order.

***(b)*** **Network Operations:** It includes proper **functioning of network operations** & **monitoring performance of network communication channels, network devices & network programs / files**. Data may be lost / corrupted through component failure. Primary components in communication sub-systems:
- **Communication lines** - Twisted pair, coaxial cables, fiber optics, microwave & satellite etc.
- **Hardware** – Ports, modems, multiplexers, switches & concentrators etc.
- **Software** – Packet switching software, polling software, data compression software etc.
- Due to **component failure**, **transmission b/w sender & receiver may be disrupted, destroyed or corrupted** in the communication system.

***(c)*** Data Preparation & Entry: Irrespective of whether the data is obtained indirectly from source documents or directly from customers, keyboard environments & facilities should be designed to promote speed & accuracy and to maintain the well-being of keyboard operators.

***(d)*** **Production Control:** It includes major functions like- **receipt & dispatch of input & output**; **job scheduling**; management of **service-level agreements** with users; **transfer pricing/charge-out control**; and **acquisition of computer consumables**.

***(e)*** **File Library:** It includes the management of an **organization's machine-readable storage media** like magnetic tapes, cartridges, & optical disks, etc.

***(f)*** **Documentation & Program Library:** It ensure that documentation is stored securely; only authorized personnel can gain access; is kept up-to-date & adequate backup exists for documentation. Documentation may include:
- **Reporting of responsibility, authority & objectives of each function** - Each IS function must be clearly defined & documented including system software, application software, database administration etc.
- **Policies & procedures**: Policies establish rules / boundaries of authority delegated to individuals. Procedures establish instructions that individuals must follow. **Documented policies** should exist in IS **for use of IS resource; Physical security; Data security; On-line security; Use of IS; Reviewing, evaluating & purchasing hardware & software; system development methodology; and Application program changes.**
- **Job descriptions** communicate management's specific expectations for job performance. **Job procedures** establish instructions on how to do job.
- **Segregation of duties** refers to distribution of work responsibilities. Individual employees are performing only stipulated duties w.r.t. their jobs.

***(g)*** **Help Desk/Technical support:** It **assists end-users** to employ end-user hardware & software such as micro-computers, spreadsheet packages, database management packages etc. and **also provides technical support** for production systems by assisting with problem resolution.

***(h)*** **Capacity Planning & Performance Monitoring: Regular performance monitoring *facilitates* the capacity planning** wherein the **resource deficiencies** must be **identified well in time** so that they can be **made available when they are needed**.

***(i)*** **Management of Outsourced Operations:** Responsibility for carrying out **day-to-day monitoring of the outsourcing contract**.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**Application Controls:** Programmatic routines within application program code with objective to ensure that data remains complete, accurate & valid during its input, update & storage.

**Boundary**
Establish interface b/w user & system.

Major controls of boundary system are access control mechanisms, which links authentic users to authorized resources, they are permitted to access.
**Access control mechanism has 3 steps** of **identification, authentication & authorization**.

**Cryptography:** A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) that are meaningless to anyone, who does not possess authentication to access respective system resource or file.
Techniques of cryptography
- **Transposition** (permute order of characters within set of data),
- **Substitution** (replace text with key-text)
- **Product cipher** (combination of transposition & substitution).

**Passwords:** An authentication mechanism with personal characteristics like name, birth date, employee code or combination of two or more can be used as password boundary access control.
Best practices followed to avoid failures;
- Minimum password length,
- Avoid usage of common words,
- Periodic change of passwords,
- Hashing of passwords &
- Number of entry attempts.

**Personal Identification Numbers (PIN):** Similar to password assigned to a user by an institution or a customer selected number.
PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission & storage.

**Identification Cards:** It store information required in an authentication process. These cards are controlled through adequate application, preparation, issue, use & card return / termination process.

**Biometric Devices:** Biometric identification are also used as boundary control techniques. e.g. finger print, eye retina etc.

**Input**
Capture, prepare and enter commands & data into system.

These controls are responsible for ensuring the accuracy & completeness of data & instruction input into application system.
Input controls are important since substantial time is spent on input of data, involve human intervention and are, therefore error & fraud prone.

**Source Document Controls:**
In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from org.
E.g. an individual with access to purchase orders & receiving reports could fabricate a purchase transaction to a non-existent supplier. If these documents entered into system with fictitious vendor's invoice, system will process it like a legitimate transaction & will create an account payable & subsequently write a cheque for payment.

To control this type of exposure:
- **Use pre-numbered source documents**
- **Use source documents in sequence**
- **Periodically audit source documents –** Missing / voided (due to error) source documents should be identified by reconciling document sequence numbers.

**Data Coding Controls:**
2 types of errors can corrupt a data code & cause processing errors.
- **Transcription Errors (3 types)**

Addition errors – Extra digit / character is added.
832 recorded as 8322.

Truncation errors - digit / character is removed from end.
832 recorded as 83.

Substitution errors - replacement of one digit with another.
832 recorded as 822.
- **Transposition Errors (2 types)**

Single transposition errors - two adjacent digits are reversed.
1234 recorded as 2134.

Multiple transposition errors - nonadjacent digits are transposed. 1234 recorded as 3241.

**Batch Controls:**
Batching is process of grouping together transactions that bear some type of relationship to each other.
Various controls can be exercises over batch to prevent or detect errors or irregularities.

| **Control Totals on Logical / Physical Batch** |
|---|
| **Financial totals -** Grand total for each field containing amounts. |
| **Hash totals -** Grand total for document in batch, e.g. source doc. serial no. can be totaled. |
| **Document/Record Counts -** Grand total for no. of doc. in batch. |

- **Physical Controls:**

Totals can be written on batch cover sheet & keyed into application system prior entry of transactions in batch. After entering all transactions in batch, system compares computed total against entered total & signals any discrepancy.
- **Logical batch:**

Person entering data must keep an independent record of transactions entered into application system. Batch totals calculated by system should be compared against batch totals calculated on the basis of these independent records.

**Validation Controls:** Input validation controls are intended to detect errors in transaction data before the data are processed.
**3 levels of input validation controls**:

**Field Interrogation:** It is programmed procedures to examine characters of data in field.
**Limit Check:** Predefined limits. E.g. PAN - 10 characters.
**Picture Checks:** Prevent processing of incorrect/invalid characters. E.g. Last character of PAN cannot be numeric.
**Valid Code Checks:** Codes / tables may be embedded in programs or stored in (direct access) files to ensure validity of input data. E.g. Assessment code while paying income tax.
**Check Digit:** Located in code as prefix, suffix, or in middle. E.g. Debit card validation, first 4 digit of visa card.
**Arithmetic Checks:** Simple arithmetic performed in different ways to validate result.
**Cross Checks:** To verify fields connected with different records tally with each other.

**Record Interrogation**
**Reasonableness Check:** Value specified in field is reasonable?
**Valid Sign:** Contents of field may determine which sign is valid for numeric field. E.g. Dollar sign.
**Sequence Check:** Physical records follow order matching with logical records. E.g. data sequentially updated in transaction file.

**File Interrogation**
**Version Usage**: Use updated version of file for processing data.
**Internal & External Labeling:** To ensure - proper files are loaded for process. External labeling is important in manual process.
**Data File Security:** To ensure CIA, prevent unauthorized access to data file. It also ensure that correct file is being processed.
**Before & after Image and Logging:** It enables re-constructing the data file back to its last state of integrity by way of rolling backward or forward of incremental transactions/events.
**File Updating & Maintenance Authorization:** To ensure that stored data are protected.
**Parity Check:** Additional controls are needed during transmission of data/program.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**Communication**
Transmit data among subsystems & systems.

**3 types of exposure** may arise.
**1**. Transmission impairments can cause difference b/w data sent & received;
**2**. Data can be lost or corrupted through component failure; &
**3**. A hostile party can subvert data that is transmitted through subsystem.

**(a) Physical Component Controls:**

| Transmission Media | Communication Lines | Modem | Port Protection Devices | Multiplexers & Concentrators |
|---|---|---|---|---|
| Path along which signal can be transmitted b/w sender & receiver. **Types**: **Guided/Bound Media** - signals are transported via physical path. E.g. twisted pair, coaxial cable, optical fiber etc. **Unguided Media** - signals propagate via free-space emission. E.g. satellite microwave, radio frequency, infrared etc. | Reliability of data transmission can be improved by choosing private (leased) communication line rather than public communication line. | - Increase data transmission speed over a communication line. - Reduces number of line errors that arise through noise, distortion. | - Used to mitigate exposures associated with dial-up access to computer system. - It performs various security functions to authenticate users. | It helps to use bandwidth/capacity of communication line more effectively. It shares use of high-cost transmission line among many messages arriving at multiplexer / concentration point from multiple low cost transmission lines. |

**(b) Line Error Control:** When data is transmitted over communication line, such data can be received in error because of distortion or noise that occurs on line. These **errors** must be **detected** & **corrected**.

**(c) Flow Controls:** It is needed because 2 nodes in a network can differ in terms of rate at which they can send, received & process data. E.g. microcomputer cannot display data on its screen at same rate at which data arrives from main frame, moreover microcomputer will have limited buffer space. Flow controls will prevent microcomputer from being overloaded & data lost.

**(d) Link Controls:** In WANs, **line error control & flow control** are important functions to manage link b/w two nodes in a network. The **link management components** mainly use two common protocols **HDLC** (Higher Level Data Link control) & **SDLC** (Synchronous Data Link Control).

**(e) Topological Controls:** A communication network topology specifies location of nodes within a network, the ways in which nodes will be linked & its data transmission capabilities.

| | |
|---|---|
| **LAN Topologies** (1) privately owned networks; (2) provide high-speed communication; and (3) Confined to limited geographic areas (e.g. single floor / building / locations within few km). They are implemented using 4 basic types of topologies: (1) Bus topology, (2) Tree topology, (3) Ring topology, and (4) Star topology. Hybrid topologies like star-ring topology & star-bus topology are also used. | **WAN Topologies:** ○ often encompass components that are owned by other parties (e.g. telephone co,); ○ provide relatively low-speed communication; & ○ span large geographic areas |

**(f) Channel Access Controls:** Two different nodes in a network can compete to use a communication channel.

- **Polling:** Polling (non contention) techniques establish an order in which a node can gain access to channel capacity.
- **Contention Methods:** Nodes in a network must compete with each other to gain access to a channel.

**(g) Internetworking Controls:** Internetworking is process of connecting 2 or more communication networks together to allow users of one network to communicate with users of other networks. They might or might not employ the same underlying hardware-software platform.

| Bridge | Router | Gateway |
|---|---|---|
| Connects similar LAN (e.g. one token ring network to another token ring network). | Performs all functions of bridge & also can connect dissimilar LAN (e.g. a bus network to a token ring network) and direct network traffic over fastest route b/w 2 nodes. | Most complex of 3 network connection devices. Its primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another. |

**Processing**
Perform decision making, computation, classification, ordering & summarization of data in system.

The processing subsystem is responsible for computing, sorting, classifying & summarizing data.
Its major **components** are **Central Processor** in which programs are executed, **real or virtual memory** in which program instructions & data are stored, **OS** that manages system resources, & **application programs** that execute instructions to achieve specific user requirements.

**(i) Processor Controls:** Processor has 3 components:
(a) **A Control unit**, which fetches programs from memory & determines their type;
(b) **an Arithmetic & Logical Unit**, which performs operations; and
(c) **Registers**, used to store temporary results & control information.

| (4 Types) Controls used to reduce expected losses from errors & irregularities associated with Central Processors **i.e. OS control** | |
|---|---|
| **Error detection & correction** | e.g. Design errors, Manufacturing defects, damage, electromagnetic interference, etc. |
| **Multiple execution states** | To determine number of & nature of execution states enforced by processor. It helps auditor to determine which user processes will be able to carry out unauthorized activities e.g. gaining access to sensitive data. (Explanation - Several processes may be associated with same program, hence opening up of 1 program often result in execution of more than 1 process) |
| **Timing Controls** | In absence of any control, program will retain use of processor & prevent other program from undertaking their work, and OS might get stuck in an infinite loop. |
| **Component Replication** | If processor failure is permanent. |

**(ii) Real Memory Controls:** This comprises fixed amount of primary storage in which programs or data reside for execution by central processor. It detect & correct errors that occur in memory cells and protect areas of memory assigned to a program from illegal access by another program.

**(iii) Virtual Memory Controls:** Virtual Memory exists when addressable storage space is larger than available real memory space. A control mechanism must be in place to maps virtual memory address into real memory address.

**(iv) Data Processing Controls:** It perform validation checks to identify errors during processing of data to ensure completeness & accuracy of data being processed. Normally, processing controls are enforced through database management system that stores data. However, adequate controls should be enforced through front end application system also.

- **Run-to-run Totals:** E.g. if current balance of invoice ledger is ` 150 & additional invoices for the period is ` 20 then total sales value should be ` 170.
- **Reasonableness Verification:** Two or more fields can be compared & cross verified to ensure their correctness.
  E.g. statutory % of provident fund can be calculated on gross pay amount to verify that the PF contribution deducted is accurate.
- **Edit Checks:** Edit checks similar to data validation controls can also be used at the processing stage to verify accuracy & completeness of data.
- **Field Initialization:** Setting all values to zero/blank before inserting the field or record.
- **Exception Reports:** It reports transaction code, why a transaction was not processed or what is error in processing the transaction.
  E.g. while processing a journal entry if only debit entry was updated & credit entry was not updated due to absence of one of important fields, then exception report would give detail why it was not updated or processed.

**Database**
Define, add, access, modify & delete data in system

Protect integrity of database when application software acts as interface to interact b/w user & database.

**Update Control**

- **Sequence Check b/w Transaction & Master Files:** Synchronization & correct sequence of processing b/w master file & transaction file is critical to maintain integrity of updating, insertion or deletion of records in master file w.r.t. transaction records.
- **Ensure All Records on Files are processed:** While processing, transaction file records mapped to respective master file, & end-of-file of transaction file w.r.t. end-of-file of master file must be ensured.
- **Process multiple transactions for single record in correct order:** Multiple transactions can occur based on a single master record (e.g. dispatch of product to different places). Here, transactions must be processed in order based on the sorted transaction codes.
- **Maintain a suspense account:** When mapping b/w master record to transaction record results in mismatch; then such transactions are maintained in suspense account. A non-zero balance in suspense A/c reflects the errors to be corrected.

**Report controls**

- **Standing Data:** Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc. Any changes or errors in these tables would have an adverse effect. Hence, it is critical to maintain their integrity. Periodic monitoring by manual checking or calculation is mandatory.
- **Print-Run-to Run control Totals:** It helps in identifying errors or irregularities like record dropped erroneously, wrong sequence of updating or application software processing errors.
- **Print Suspense Account Entries:** Similar to update controls, suspense A/c entries are periodically monitored with respective error & action taken on time.
- **Existence/Recovery Controls:** Back-up & recovery strategies together encompass the controls required to restore database. Backup strategies are implemented using prior version & logs of transactions or changes to database. Recovery strategies involve roll-forward (current state database from previous version) or roll-backward (previous state database from current version) methods.

**Output**
Retrieve & present data to users of system

To ensure - data delivered to users will be presented, formatted & delivered in consistent & secured manner.
Output can be in any form e.g. printed data or database file in removable media. It should ensure confidentiality & integrity of output is maintained.

- **Storage & logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal & usage. Only authorized persons should be allowed access to stationery supplies. E.g. security forms, negotiable instruments, etc.
- **Logging of output program executions:** When 'programs used for output of data' are executed, these should be logged & monitored; otherwise confidentiality & integrity of data may be compromised.
- **Spooling/queuing:** Spool – "Simultaneous Peripherals Operations Online". It ensure - user is able to continue working, while the print operation is getting completed. When a file is to be printed, OS stores the data stream to be sent to printer in temporary file on hard disk. This file is then "spooled" to the printer as soon as the printer is ready. Queue - list of documents waiting to be printed on a particular printer; this should not be subject to unauthorized modifications.
- **Controls over printing:** Outputs should be made on the correct printer & it should be ensured that unauthorized disclosure of information printed does not take place. Users must be trained to select the correct printer & access restrictions may be placed on the workstations that can be used for printing.
- **Report distribution & collection controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. Distributed & collected immediately after printing to ensure that time gap b/w generation & distribution is reduced. Maintain log of reports generated & to whom these were distributed. Where users have to collect reports, the user should be responsible for timely collection of report, especially if it is printed in a public area. Maintain log of reports printed & collected. Uncollected reports should be stored securely.
- **Retention controls:** It consider the duration for which outputs should be retained before being destroyed. Consider type of medium on which output is stored. Date should be determined for each output item produced. Various factors like need & use of output, legislative requirements affect the retention period.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**Information Technology General Controls (ITGC)** are the basic policies & procedures which ensure that an organization's IS are properly safeguarded, application programs & data are secure, and computerized operations can be recovered in case of unexpected interruptions. ITGC are the foundation for overall IT control environment as they provide assurance that systems operate as intended & that output is reliable. Failure to ensure these controls are designed & operating effectively means that there will not be any assurance over the IT Application Controls.

**Controls over Data Integrity & Security**

**Classification of information & documents (classification into an appropriate sensitivity level)**

- **Top Secret:** Highly sensitive internal information e.g. pending mergers / acquisitions; investment strategies; plans / designs; that could seriously damage the organization if such information were lost or made public. It has very restricted distribution & must be protected at all times. **Security** at this level should be the **highest possible**.
- **Highly Confidential:** Information that, if made public or even shared around the organization, could seriously impede organization's operations & is considered critical to its ongoing operations. Information would include accounting information, sensitive customer information of banks / solicitors / accountants, patient's medical records & similar highly sensitive data. It should not be copied or removed from organization's operational control without specific authority. **Security** at this level should be **very high**.
- **Proprietary:** Information of a proprietary nature; procedures, operational work routines, project plans, designs & specifications *which define the way in which organization operates*. Such information is normally for proprietary use to authorized personnel only. **Security** at this level should be **high**.
- **Internal Use only:** Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. E.g. internal memos, minutes, internal project reports. **Security** at this level should **controlled but normal**.
- **Public Documents:** Information in public domain; annual reports, press statements etc.; which has been approved for public use. **Security** at this level should **minimal**.

**Data Integrity:** It is reflection of the accuracy, correctness, validity, & currency of the data.

**Primary objective of data integrity control techniques**

- To *prevent, detect & correct errors in transactions* as they flow through various stages of a specific date processing program.
- It *ensure the integrity* of specific application's inputs, stored data, programs, data transmissions & outputs.
- It *protect data* from *accidental or malicious alteration or destruction* & *provide assurance* to user that *information meets expectations about its quality & integrity*.

**Assessing data integrity** involves evaluating the following critical procedures:

- *Virus detection & elimination software* is installed & activated.
- *Data integrity & validation controls* are used to provide assurance that *information has not been altered & system functions as intended.*

**Data Integrity Controls**

| Control Category | Source data control | Input validation routines | On-line data entry controls | Data processing & storage controls | Output controls | Data transmission controls |
|---|---|---|---|---|---|---|
| **Threats / Risks** | Invalid, incomplete, or inaccurate source data input | Invalid or inaccurate data in computer-processed transaction files | Invalid or inaccurate transaction input entered through on-line terminals | Inaccurate or incomplete data in computer-processed master files | Inaccurate or incomplete computer output | Unauthorized access to data being transmitted or system failures causing errors in data transmission. |
| **Controls** | 1. Design Form<br>2. Pre-numbered Form<br>3. Cancellation & Storage of Documents<br>4. Authorisation of Source Documents<br>5. Segregation of Duties<br>6. Check-Digit verification | 1. Edit Check – Sequence/ Field/ Validity/ Limit/ Range check etc.<br>2. Enter exceptions in an error log; investigate, correct & resubmit them; re-edit them.<br>3. Summary error report. | 1. Field/ Limit/ Range/ Validity & redundant data check, etc.<br>2. User-IDs & Password<br>3. Compatibility tests<br>4. Automatic Date<br>5. Pre-formatting<br>6. Completeness test<br>7. Transaction Log<br>8. Clear error messages | 1. Policies & procedures w.r.t. data processing, storage, data security, confidentiality, audit trails.<br>2. Monitoring data entry<br>3. Reconciliation of database totals with externally maintained totals<br>4. Exception reporting<br>5. Protection against conditions that could harm stored data<br>6. Use of file labels<br>7. Adequate Backup | 1. Procedures to ensure that system outputs conform to organization's integrity objectives, policies, and standards,<br>2. Reconciliation of batch totals,<br>3. Proper distribution of output,<br>4. Confidential outputs being delivered are protected from unauthorized access, modification & misrouting<br>5. Sensitive or confidential output stored in secure area,<br>6. Error & exception reports. | 1. Monitor network to detect week points<br>2. Design network to handle peak processing<br>3. Multiple communication paths between network components<br>4. Preventive maintenance<br>5. Data encryption<br>6. Routing verification<br>7. Message acknowledgement |

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**Data Integrity Policies**

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments** into Development, Test & Production is required for critical systems.
- **Offsite Backup Storage:** Backups older than 1 month must be sent offsite for permanent storage.
- **Quarter-End & Year-End Backups** must be done separately from normal schedule, for accounting purposes
- **Disaster Recovery:** DRP must be used to ensure continuity of corporate business in the event of an outage.

**Data Security**

Data security encompasses the protection / prevention of data against accidental or intentional unauthorized disclosure, modification & deletion. Multiple levels of data security are necessary in an IS environment.

*An IS auditor is responsible to evaluate the following while reviewing the adequacy of data security controls*:

- Who is responsible for the accuracy of data?
- Who is permitted to update data?
- Who is permitted to read & use data?
- Who is responsible for determining who can read & update data?
- Who controls the security of data?
- If the IS system is outsourced, what security controls & protection mechanism does the vendor have in place to secure & protect data?
- Contractually, what penalties or remedies are in place to protect the tangible & intangible values of information?
- Disclosure of sensitive information is a serious concern to organization & is mandatory on auditor's list of priorities.

**Financial Controls**

These controls are generally defined as procedures exercised by system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, items counts & amount of transactions for settlement of transaction of transaction processed & reconciliation of the applications (subsystem) to general ledger.

**Major Financial Control Techniques:**

- **Authorization:** It means obtaining the authority to perform some act typically accessing to such assets. E.g. OTP or PIN of ATM
- **Budgets:** It estimates amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, and analyze variance to find cause & solution.
- **Cancellation of documents:** Marking a document in such a way to prevent its reuse. E.g. Marking invoices with a "paid" or "processed" stamp or punching a hole.
- **Dual control:** It means 2 people simultaneously access an asset. E.g. Depositories of banks' 24-hour teller machines should be accessed and emptied with two people present. Many people confuse dual control with dual access, but these are distinct & different. Dual access divides the access function b/w 2 people: once access is achieved, only one person handles the asset. E.g. With teller - machines, 2 tellers would open the depository vault door together, but only 1 would retrieve the deposit envelopes.
- **Input/ output verification:** It means comparing the information provided by computer system to the input documents.
- **Safekeeping:** It means physically securing assets, such as computer disks, under lock & key, in a desk drawer, file cabinet storeroom, or vault.
- **Sequentially numbered documents:** These are working documents with preprinted sequential numbers enabling detection of missing documents.
- **Supervisory review:** It means review of work by supervisor & sign-off on the documents as an evidence that supervisor had reviewed them.

**Personal Computers Controls**

**Related risks:**

- PC are small in size & easy to connect & disconnect, may be taken outside organization for theft of information.
- Pen drives / Hard disks can be easily transported from one place to another resulting of which data theft may occur.
- PC is basically a single user oriented machine & hence, does not provide inherent data safeguards.
- Computer viruses & pirated software may result in data corruption, slow operations & system break down etc.
- Segregation of duty is not possible, owing to limited number of staff.
- Leakage of information due to higher staff mobility.
- Operating staff may not be adequately trained.
- Weak access control.

**Security Measures:**

- Physically locking the system;
- Proper logging of equipment shifting must be done;
- Centralized purchase of hardware & software;
- Standards set for developing, testing & documenting;
- Uses of antimalware / antivirus software;
- Control on use of PC & their peripheral; and
- Use of disc locks to prevent unauthorized access to floppy disk or pen drive of a computer.

# CHAPTER – 3 PROTECTION OF INFORMATION SYSTEM

**Cyber Frauds**

With advancements in the technology, cyber frauds are also increasing day-by-day across the world. Major reasons behind the rise of such frauds:

- Failure of internal control system,
- Failure of organizations to update themselves to new set of risk, and
- Smart fraudsters: People who are able to target the weaknesses in system, lacunae's (gaps/holes) in internal controls, even before organization realizes that such gaps are there.

SA 240 (Revised) defines fraud as "intentional misrepresentation of financial information by one or more individuals among employees, management, TCWG, or third parties." Fraud has also been defined as "Intentional Error". **Cyber Fraud** means fraud committed by use of technology. Cyber fraud refers to any type of deliberate deception for unfair / unlawful gain that occurs online. E.g. online credit card theft, non-delivery of paid products purchased online, etc.

**On the basis of functionality, these are of 2 types:**

- **Pure Cyber Frauds:** Frauds, which exists only in cyber world. They are borne out of use of technology. E.g. Website hacking.
- **Cyber Enabled Frauds:** Frauds, which can be committed in physical world also but with use of technology. E.g. Withdrawal of money from bank account by stealing PIN numbers.

Fraudster may be from within the organization or from outside the organization. It has been observed that the most of cyber frauds include a person from within the organization.

**Cyber Attacks**

- **Phishing:** It is act of attempting to acquire information such as usernames, passwords & credit card details (& sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.
- **Network Scanning**: It is process to identify active hosts of a system for getting information about IP addresses etc.
- **Virus/Malicious Code**: Section 43 of IT Act "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;
- **Spam**: E-mailing same message to everyone on Usenet News Group is termed as spam.
- **Website Compromise / Malware Propagation**: It includes website defacements. Hosting malware on websites in an unauthorized manner.
- **Others:** These are given as follows:
  - **Cracking:** Crackers are hackers with malicious intentions.
  - **Eavesdropping:** Listening of private voice or data transmissions, often using a wiretap.
  - **E-mail Forgery:** Sending e-mail messages that look as if someone else sent it.
  - **E-mail Threats:** Sending a threatening message to try & get recipient to do something that would make it possible to defraud him.
  - **Scavenging:** Gaining access to confidential information by searching corporate records.

**Impact of Cyber Frauds on Enterprises**

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. E.g. wrongfully withdrawal of money from bank accounts.
- **Legal Repercussions:** Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of IT Act, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- **Loss of credibility or Competitive Edge:** News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility. E.g. share prices of companies went down, as the news of cyber-attack spread to the market.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. E.g. Instances of individuals leaking information about governments' secret programs.
- **Sabotage:** The above situation may lead to misuse of such information by enemy country.

**Techniques to Commit Cyber Frauds**

- **Hacking:** It refers to unauthorized access & use of computer systems, usually by means of PC & a telecommunication network. Normally, hackers do not intend to cause any damage.
- **Cracking:** Crackers are hackers with malicious intentions, which means, un-authorized entry. Hacking is a general term, with two nomenclatures namely: Ethical & Un-ethical hacking. Un-ethical hacking is classified as Cracking.
- **Data Diddling:** Changing data before, during, or after it is entered into system in order to delete, alter data.
- **Data Leakage:** It refers to unauthorized copying of company data such as computer files.
- **Denial of Service (DoS) Attack:** It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of system from functioning.
- **Internet Terrorism:** It refers to using Internet to disrupt electronic commerce and to destroy company and individual communications.
- **Logic Time Bombs:** These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- **Masquerading or Impersonation:** In this case, perpetrator gains access to system by pretending to be an authorized user.
- **Password Cracking:** Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them & then uses them to gain access to system resources such as programs, files & data.
- **Piggybacking:** It refers to tapping into a telecommunication line & latching on to a legitimate user before s/he logs into system.
- **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- **Scavenging or Dumpster Diving:** It refers to gaining access to confidential information by searching corporate records.
- **Social Engineering Techniques:** In this case, perpetrator tricks an employee to give out the information needed to get into system.
- **Super Zapping:** It refers to unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
- **Trap Door:** In this technique, perpetrator enters in system using a back door that bypasses normal system controls and perpetrates fraud.

# CHAPTER – 4 BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

**BCM policy** defines **processes of setting up activities for establishing business continuity capability & ongoing management & maintenance of business continuity capability**. The set-up activities incorporate specification, end-to-end design, build, implementation & initial exercising of business continuity capability. The ongoing maintenance & management activities include embedding business continuity within enterprise, exercising plans regularly & updating & communicating them, particularly when there is significant change in premises, personnel, process market, technology or organizational structure.

**Objective of BCM Policy**

- To minimize/eliminate loss of revenue / reputation / productivity & customer satisfaction.
- To identify critical services & activities.
- To ensure continuity of delivery of key service after business disruption caused by disaster.
- To manage invocation of incident & BCP.
- To test, revise, update Incident Management Plans & BCP.
- To assign responsibility of planning & management to relevant senior management.

**BCM** is an effective management process to help enterprise to manage disruption by assessing potential threats, managing consequences of disruption and reducing & eliminating losses that could occur. For effective implementation of BCM, enterprises should conduct regular & independent internal audit & take corrective actions on findings of auditor.

**Need of BCM**

Business continuity means maintaining uninterrupted availability of all key business resources required to support essential business activities.

To meet business objectives & ensure continuity of services & operations, an enterprise shall adapt & follow well-defined & time-tested plans & procedures, build redundancy in teams & infrastructure, manage quick & efficient transition to backup arrangement for business systems & services.

**Key terms related to BCM**

- **Business Contingency:** It is event with potential to disrupt computer operations, by disrupting critical activities & business functions like power outage, hardware failure, fire, or storm. Most destructive event is called disaster.
- **BCP Process:** BCP is process designed to reduce risk of unexpected disruption of its critical functions, & assure continuity of minimum level of services necessary for critical operations. It ensure that vital business functions (critical business operations) are recovered & operationalized within acceptable timeframe. It ensure continuity of business & not the continuity of all systems. It identifies critical functions & resources required to support them & provides guidelines for ensuring that needed personnel & resources are available for timely restoration of services.
- **BCP**: It refers to ability of enterprises to recover from disaster & continue operations with least impact. It is not enough to have BCP, enterprise must have independent audit of BCP to confirm its adequacy & appropriateness.

**Advantages of BCM**

- Proactively assess threat scenario & potential risks
- Planned response to disruptions to minimize impact on enterprise
- Demonstrate a response through a process of regular testing & trainings

**BCP** is creation & validation of practical logistical plan for enterprise to recover & restore critical (urgent) functions within predetermined time after disaster / disruption. It is to be performed before disaster occurs otherwise it would be too late to plan effective response. Consequences of disaster may be more severe in case of inadequate planning / no planning on operations, profitability, quality of service, & convenience.

During disruptive events, BCP is guiding document which layout steps to be initiated by mgmt. to continue operations / run business under stressful condition on occurrence of disaster.

**Areas covered under BCP**

- **Business Resumption Planning:** It is operation's piece of BCP to resume business.
- **Disaster Recovery Planning:** It is technological aspect of BCP for advance planning & preparation necessary to ensure continuity of critical business functions in event of disaster.
- **Crisis Management:** It means co-ordination of org.'s response to crisis to minimize damage to its profitability, reputation or ability to operate.

**Objectives of BCP**

Primary objective is to minimize loss by minimizing cost associated with disruptions & enable org. to survive disaster & to re-establish normal business operations. Key objectives of plan shall include:

- Provide safety of people on premises during disaster;
- Identify critical lines of business & supporting functions.
- Continue critical business operations;
- Minimize duration of serious disruption
- Minimize immediate damage & losses;
- Establish management succession & emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce complexity of recovery effort;

**Goals of BCP**

- Identify weaknesses & implement disaster prevention program;
- minimize duration of disruption to business operations;
- facilitate effective co-ordination of recovery tasks;
- reduce complexity of recovery effort.

**Methodology/ Characteristics**

- Providing management with detailed understanding of efforts required to develop & maintain effective recovery plan.
- Obtaining commitment from appropriate management to support & participate in effort.
- Defining recovery requirements from perspective of business functions.
- Documenting impact of loss to operations & key business functions.
- Focusing appropriately on disaster prevention, impact minimization & orderly recovery.
- Selecting business continuity teams.
- Developing business continuity plan which is understandable, easy to use & maintain.
- Define how business continuity considerations must be integrated into ongoing business planning & system development processes so that plan remains viable.

**BCP Manual**

BCP manual is documented description of actions to be taken, resources to be used & procedures to be followed before, during & after event which disrupt business operations. BCP is expected to provide:

- Reasonable assurance to senior management about capability to recover from unexpected incident / disaster & continue to provide services with minimum impact.
- Anticipate various types of incident / disaster scenarios & outline action plan for recovering from same with minimum impact & ensuring 'Continuous availability of all key services to clients'.
- Specify responsibility of BCM team is to establish appropriate BCP procedures to ensure continuity of critical business function.



(rajveer.an.indian@gmail.com)

# CHAPTER – 4 BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

**Eight-Phases**

- **Phase 1 – Pre-Planning Activities (BCP Initiation)**
  It **obtain understanding of existing & projected computing environment** of org. **to identify & address any issues** that could **have impact on project**.
  In this phase, a **Steering Committee is established** to provide direction & guidance to project team & also make all decisions related to recovery planning effort.
- **Phase 2 – Vulnerability Assessment & General Definition of Requirements**
  Security & controls within org. are continuing concern. It is better to **concentrate on activities having effect of reducing the possibility of disaster occurrence, rather than concentrating on minimizing impact of actual disaster**.
  a. A **thorough Security Assessment of system & communications environment** like physical security, operating procedures, backup & contingency planning, systems development & maintenance, database security etc.
  b. Security Assessment will **enable** project team to **improve existing / implement emergency plans & disaster prevention measures**.
  c. **Findings & recommendations** should be **forwarded to the Steering Committee** so that corrective actions can be initiated.
  d. Assemble Project Team & **conduct awareness sessions**.
- **Phase 3 – Business Impact Analysis (BIA):** It enables the project team to:
  a. **identify critical systems, processes & functions**;
  b. **assess economic impact** of incidents & disasters which result in **denial of access to systems services & facilities**; &
  c. **assess "pain threshold**," i.e. length of time which business units can survive without access to systems, services & facilities.
  **BIA Report** should be **presented to Steering Committee**. BIA report **identifies critical service functions & timeframes** in which they must be recovered after interruption
- **Phase 4 – Detailed Definition of Requirements**
  In this phase, a **profile of recovery requirements is developed for analyzing alternative recovery strategies**. The profile is developed **by identifying resources required to support critical functions identified in Phase 3**. Profile include hardware, software, documentation, facilities & personnel for each business unit.
- **Phase 5 – Plan Development**
  Objective of this phase is to **determine available options**. It **formulates alternative operating strategies** for providing timely recovery of all critical processes. In this phase, **recovery plans components are defined & plans are documented**.
- **Phase 6 – Testing/Exercising Program**
  Testing/Exercising Programs are developed during this phase. Testing/exercising goals are established & alternative testing strategies are evaluated. **Testing strategies suitable to environment should be selected & on-going testing program should be established**.
- **Phase 7 – Maintenance Program**
  Maintenance of plans is critical for success of actual recovery. **Management should revised / implemented to take recovery plan maintenance into account**.
- **Phase 8 – Initial Plan Testing & Plan Implementation:**
  **Once plans are developed, initial tests of plans are conducted & necessary modifications to plans are made based on analysis of test results**. This phase include :
  a. Defining **test purpose/approach**
  b. Identifying **test teams**
  c. **Structuring** test
  d. **Conducting** test
  e. Analyzing **test results**
  f. **Modifying** plan as appropriate

| **COMPONENTS OF BCM PROCESS** | |
|---|---|
| **Management Process** | The management process enables business continuity, capacity & capability to be established & maintained as per enterprise requirement. |
| | **Organisation Structure:** Organisation should nominate a person / team with **appropriate authority to be accountable for BCM policy implementation & maintenance & their responsibilities should be clearly defined.** |
| | **Implementing Business Continuity in Enterprise & Maintenance:** Top management should **appoint BCM Manager responsible for BCM policy & its implementation supported by each function**. Manager from each function represent their areas of operation & they are also responsible for ongoing operation & maintenance of system within their area of responsibility. Training may be required to some staff to effectively carry out their BCM responsibilities. |
| | **Activities in Implementation:**<br>• Define **scope, roles & responsibilities**<br>• **Engage & Involve all stakeholders**<br>• **Testing** of program on regular basis<br>• Manage **Cost Benefit**<br>• **Review, Rework & Update** Business Capability, RA, BIA<br>• Convert **Policies into Strategies** |
| | **Documentation:** Following documents are part of BCM system:<br>• Business continuity **policy, plan & strategies**;<br>• Business impact analysis **(BIA) report**;<br>• **Risk assessment report**;<br>• Aims & **objectives** of each function;<br>• **Activities undertaken** by each function;<br>• **Change** control**, preventative** action**, corrective** action**, document & record control** processes**;**<br>• **Exercise schedule & results**;<br>• **Incident log**<br>• **Training program.**<br>Documents for **statutory, regulatory or customer requirement** should be retained for dictated period, **minimum 1 year**. It includes references to **all business interruptions & incidents**, irrespective of nature & length of disruption. |


(rajveer.an.indian@gmail.com)

# CHAPTER – 4 BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

<table>
<tr><td rowspan="4">Information Collection Process</td><td>Assessment process help to prioritize enterprise's products, services & urgency of activities that are required to be delivered. It will helps in selection of appropriate BCM strategies in next process.<br>To design an effective BCM, it is pertinent to understand:<br>• enterprise's objectives, stakeholder obligations, statutory duties & environment in which enterprise operates;<br>• activities, assets & resources which support delivery of these products & services;<br>• impact & consequences of failure of these activities, assets & resources; &<br>• Perceived threats that could disrupt enterprise's key products & services & critical activities, assets & resources.</td></tr>
<tr><td>Business Impact Analysis (BIA) means systematically assessing potential impacts of disruption of activities that support key product & services. It helps :<br>• To identify critical systems, processes & functions<br>• Assess economic impact of incidents & disasters that result in denial of access to system, services & facilities<br>• Assess "pain threshold", i.e. length of time that business units can survive without access to system, services & facilities.<br>For each activity supporting delivery of key products & services, enterprise should:<br>• assess impacts that would occur if the activity was disrupted over a period of time;<br>• identify maximum time period within which such activity needs to be resumed after disruption;<br>• Identify critical business processes;<br>• assess minimum level at which activity needs to be performed on its resumption;<br>• identify length of time within which normal levels of operation need to be resumed; &<br>• Identify any inter-dependent activities, assets, supporting infrastructure or resources which have also to be maintained continuously or recovered.<br>Enterprise should have documented approach to conduct BIA, & should document its approach of assessing impact of disruption, its findings & conclusions.<br>BIA Report –<br>i. Presented to Top Management<br>ii. Identifies critical service functions & time frame within which they must be recovered after interruption.<br>iii. Used as a basis for identifying systems & resources required to support critical services.</td></tr>
<tr><td>Classification of Critical Activities: BIA will result in categorization (like Vital, Desirable & Essential) of infrastructure & business function following by disaster scenarios (Catastrophic, major, minor trivial) for various disaster causes (fire, flood, system failure etc.), which is given as follows:<br>Business Categorization (Vital/Essential/Desirable): Parameters to be considered:<br>○ Loss of revenue; ○ Decrease in customer satisfaction; &<br>○ Loss of reputation; ○ Loss of productivity (man-hours).<br>These parameters shall be graded in three-point scale 1-3 where,<br>1 = Low (L), 2 = Medium (M), 3 = High (H)<br>Disaster Scenarios (Major/Minor/Trivial/Catastrophic): It can be ranked & categorized based on how severe damage it can.<br>○ Trivial / Insignificant<br>○ Minor<br>○ Major<br>○ Catastrophic<br>BIA matrix is also used to assess Risk thus also referred as Risk Assessment Matrix. Risks can be place on the matrix on the basis of:<br>Likelihood: Probability of risk or Occurrence of disaster<br>○ Definite – Almost Certain (+80%)<br>○ Likely – 60-80%<br>○ Unlikely – Rare & exceptional (-10%)<br>Consequences: Severity of impact or Extent of damage that can be caused by risk<br>○ Trivial / Insignificant – Near negligible amount of damage<br>○ Minor – Some damage but not too significant<br>○ Major – Significantly large consequences leading to great amount of loss i.e. critical<br>○ Catastrophic – Make project completely unproductive & Unfruitful, it must be of top priority.</td></tr>
<tr><td>Risk Assessment (To decide priority of risks):<br>It is assessment of disruption to critical activities. Enterprise should determine threats & vulnerabilities & its impact, if it becomes a reality.<br>Threats - fire, flood, power failure, staff loss, staff absenteeism, computer viruses or hardware failure.<br>Vulnerabilities - weaknesses that can be exploited by threats, e.g. single points of failure, inadequacies in fire protection.<br>It helps to improve / implement emergency plans. With help of BIA & risk assessment, identify measures that:<br>○ reduce likelihood of disruption;<br>○ shorten period of disruption; &<br>○ limit impact of disruption on enterprise's key products & services.</td></tr>
<tr><td>Strategy Process</td><td>Preparation is needed to implement strategies for protecting critical functions & their supporting resources. Enterprise develops & documents series of plans to effectively manage incident having impacts & subsequently recover its critical activities & their supporting resources within agreed time. Some non-critical activity also required to be recovered as they assist critical activities to operate more efficiently & effectively. Enterprise may adopt any strategy but it should adopt that strategy which reduces likelihood of incidents & its potential impact for both critical & non-critical activities.</td></tr>
</table>


(rajveer.an.indian@gmail.com)

# CHAPTER – 4 BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

<table>
<tr><td>Development & Implementation Process</td><td colspan="2">To Implement strategy, enterprise should have an exclusive organization structure, Incident Management Team / Crisis management team for effective response & recovery from disruptions.<br>1. Incident management plan:<br>o To manage initial phase of incident<br>o Should be flexible, feasible & easy to read & understand<br>o Should have support from TOP Mgmt. with appropriate budget.<br><br>2. Business Continuity Plan: It support critical activities by recovering or maintaining such activities in event of disruption into normal business operation. Recovery strategies may be 2-tiered:<br>o Business: Logistics, accounting, human resources, etc.; &<br>o Technical: Information Technology</td></tr>
<tr><td rowspan="4">Testing & Maintenance Process</td><td colspan="2">BCM Testing: BCP should be tested periodically to remove flaws that arise in planning & implementation. Plan should be updated with passage of time & responsibility for same should be clearly defined.</td></tr>
<tr><td>BCP testing might improve BCM capability by:<br>o Practicing ability to recover from incident;<br>o Verifying - BCP incorporates all critical activities, their dependencies & priorities;<br>o Highlighting assumptions needed to be questioned;<br>o Boosting confidence amongst participants;<br>o Raising awareness of business continuity;<br>o Validating effectiveness & timeliness of restoration of critical activities;<br>o Demonstrating competence of primary response teams & their alternatives.</td><td>Testing program should be flexible, considering changes within enterprise, outcome of previous one, etc. Objectives of BCP tests are to ensure that:<br>o Recovery procedures are complete & workable.<br>o To evaluate competence of personnel in recovery procedures.<br>o Business processes, systems, personnel, facilities & data are obtainable & operational to perform recovery processes.<br>o Manual recovery procedures & IT backup systems are current & can be operational or restored.<br>o Success or failure of business continuity training program is monitored.</td></tr>
<tr><td colspan="2">Implementation: Once plans are developed, initial tests of plans are conducted & necessary modifications in plans are made based on analysis of test results, then plan are implemented.</td></tr>
<tr><td colspan="2">Maintenance: It is important to keep preparations including documentation up-to-date.<br>MAINTENANCE TASKS UNDERTAKEN IN DEVELOPMENT OF BCP: Maintenance task determine the following<br>o Ownership & responsibility for maintaining BCP strategies<br>o Identify BCP maintenance triggers to ensure that any ‘organisational, operational, & structural changes’ are communicated to personnel who are accountable for ensuring that plan remains up-to-date;<br>o Maintenance regime to ensure plan remains up-to-date;<br>o Maintenance processes to update the plan; &<br>o Implement version control procedures to ensure plan is up-to-date.</td></tr>
<tr><td colspan="2">Key areas for REVIEW OF BCM ARRANGEMENTS <u>OR</u> AUDIT / SELF-ASSESSMENT of enterprise’s BCM program:<br>o All key products & services & their supporting critical activities & resources have been identified & included in enterprise’s BCM strategy;<br>o Enterprise’s BCM policy, strategies, framework & plans accurately reflect its priorities & requirements;<br>o Enterprise’s BCM competence & its BCM capability are effective & fit-for-purpose to help management to command & control incident;<br>o Enterprise’s BCM solutions are effective, up-to-date & fit-for-purpose, & appropriate to level of risk faced by enterprise;<br>o Enterprise’s BCM maintenance & exercising programs have been effectively implemented;<br>o BCM strategies & plans incorporate improvements identified during incidents & exercises in maintenance program;<br>o Enterprise has ongoing program for BCM training & awareness;<br>o BCM procedures have been effectively communicated to relevant staff, & such staff understand their roles & responsibilities; &<br>o Change control processes are in place & operate effectively.</td></tr>
<tr><td>Training Process</td><td colspan="2">Why:<br>o To make BCM program more efficient<br>o To minimize likelihood & impact of disruption<br>o To gain confidence of stakeholders (especially staff & customer) in ability to handle disruptions.<br>BCM Culture is supported by:<br>o Involvement of Senior Personnel<br>o Assignment of Responsibilities<br>o Awareness<br>o Skill training & exercising plan<br>Training, Awareness & Competency: While developing BCM, following competencies of personnel are required:<br>o Actively listens to others;<br>o Provides support in difficult or challenging circumstances;<br>o Responds constructively to difficult circumstances;<br>o Promotes positive culture;<br>o Acknowledges contribution of colleagues;<br>o Encourages taking of calculated risks;<br>o Encourages & actively responds to new ideas;<br>o Consults & involves team members to resolve problems;<br>o Demonstrates personal integrity.</td></tr>
</table>



(rajveer.an.indian@gmail.com)

# CHAPTER – 4 BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

**TYPES OF PLAN:** THERE ARE VARIOUS KINDS OF PLAN THAT NEEDS TO BE DESIGNED.

**Emergency Plan**

It specifies immediate actions to be taken when disaster occurs. Management must identify situations that require to invoke plan e.g., major fire, structural damage, or terrorist attack.

- '**Who is to be notified** immediately when disaster occurs - management, police, fire department, medical team etc.?
- **Actions to be undertaken**, like shutdown of equipment, removal of files, or termination of power.
- **Evacuation procedures** required must be specified.
- **Return procedures** (e.g., conditions that must be met before site is considered safe) must be designated.

**Personnel responsible** for actions must be identified & **protocols to be followed** must be specified clearly.

**Back-up-plan**

It specifies type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled & operations can be restarted, personnel responsible to gather backup resources & restart operations, priorities & time frame for recovery.

- It is better to have **more than 1 knowledgeable person** in backup task in case someone leaves or injured when disaster occurs.
- **Lists of hardware & software** must be updated to reflect acquisitions & disposals.

**Recovery Plan**

- It set out **procedures to restore** full IS capabilities.
- It should identify a **recovery committee** that will be responsible for working out specifics of recovery to be undertaken.
- It should **specify responsibilities** of committee.
- It might also **indicate which applications** are to be **recovered first**.
- Periodically, they must **review & practice executing their responsibilities** so they will be prepared when disaster occur.
- If committee **members leaves**, **new** members must be **appointed** immediately.

**Test Plan**

Its purpose is **to identify deficiencies in emergency, backup, or recovery plans** or in **preparedness of org.** & its **personnel** for facing disaster.

Periodically, test plans must be invoked but unfortunately, top managers are **often unwilling to carry out it because daily operations are disrupted**. They also **fear a real disaster could arise as a result of test procedures**.

**TYPES OF BACK-UPS**

**Full Backup**

It captures all files on disk / within folder selected for backup. Every backup generated contains every file in backup set. At each backup run, all files designated in backup job will be backed up again including files & folders that have not changed.

It is commonly used as an initial / first backup followed with subsequent incremental or differential backups. Any good backup plan has at least one full backup of a server.

**Advantages**

- Easy to manage & fast restoration

**Disadvantages**

- Backup take long time & consume more storage

**Incremental Backup**

It captures files that were created or changed since last backup (full / incremental backup). With incremental backups, one full backup is done first & subsequent backup runs are just changed files & new files added since LAST BACKUP.

**Advantages**

- Faster backup
- Efficient use of storage

**Disadvantages**

- Restoration is slower & complex

**Differential Backup**

It fall in middle b/w full backups & incremental backup. It stores files that have changed since last full backup. With differential backups, one full backup is done first & subsequent backup runs are changes made since LAST FULL BACKUP.

Restoring from a differential backup is 2-step operation:

i. First restore from last full backup; & then
ii. Restore the appropriate differential backup.

**Advantages**

- Much faster backups than full backups
- More efficient use of storage than full backups
- Faster & simpler restoration than incremental backups

**Disadvantages**

- Slower backups than incremental backups
- Not as efficient use of storage as incremental backups
- Slower & complicated restoration than with full backups

**Mirror Back-up**

It's a mirror of the source being backed up. With mirror backups, when a file in source is deleted, that file is also deleted in mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through virus may also cause that same file in mirror to be deleted as well.

It is identical to a full backup with exception that files are not compressed in zip files & they cannot be protected with a password. It is used to create exact copy of backup data. E.g. - Many online backup services offer a mirror backup with 30 day delete.

**Advantages**

- Backup is clean & does not contain old & obsolete files.

**Disadvantages**

- Chances that files in source deleted accidentally / by sabotage / through virus & also deleted from backup mirror.



(rajveer.an.indian@gmail.com)

# CHAPTER – 4 BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

**ALTERNATIVE PROCESSING FACILITY ARRANGEMENTS (Backup option sites)**

| | | | |
|---|---|---|---|
| **Cold Site:** If org. can tolerate some downtime, cold-site backup might be appropriate. A cold site has **all facilities** needed to install a mainframe system like raised floors, AC, power, communication lines etc. It can be managed inhouse or outhouse. | **Hot Site:** If fast recovery is critical, org. might need hot site backup. **All hardware & operations facilities** will be available at hot site. **In some cases, software, data & supplies might also be stored there**. Hot site is expensive to maintain. They are usually shared with other organisations that have hot-site needs. | **Warm Site:** A warm site provides intermediate level of backup. It has **all cold-site facilities in addition to hardware that might be difficult to obtain or install**. E.g. a warm site might contain selected peripheral equipment plus a small mainframe with sufficient power to handle critical applications in short run. | **Reciprocal Agreement: Two or more organisations might agree to provide backup facilities to each other in event of one suffering disaster**. This option is relatively cheap, but each participant must maintain sufficient capacity to operate another's critical system. * |

***If a third-party site is to be used for backup & recovery purposes, SECURITY ADMINISTRATORS MUST ENSURE THAT A CONTRACT IS WRITTEN TO COVER ISSUES**:

- how soon site will be made available subsequent to disaster;
- number of organizations allowed to use the site concurrently in event of disaster;
- priority to be given to concurrent users of the site in event of common disaster ;
- period during which the site can be used;
- conditions under which site can be used;
- facilities & services agreed to make available; &
- What controls will be in place & working at the off-site facility.

**CONTENT OF DRP DOCUMENT**

- **Emergency procedures** to be taken after incident posing threats on business operations / human life. E.g. Police, Fire brigade.
- **Fallback procedures** for moving essential business activities to alternate temporary locations.
- **Resumption procedures** to be taken to return to normal business operations.
- **Maintenance schedule** specifying 'how & when plan will be tested'.
- **List of important vendors** including contact numbers & addresses.
- **List of phone numbers of employees** in event of emergency.
- **Emergency phone list** like fire, police, hardware, software, suppliers, customers, back-up location, etc.
- **Medical procedures** for emergency purposes.
- **Insurance papers & claim form**.
- **Location of data & program files, documentation manuals, back-up media**.
- **Names of employees trained for emergency situation**, first aid & life saving techniques with **their contact details.**
- **Details of airline, hotels & transport arrangement**.

**AUDIT OF BCP/DRP**

**General**

- **Identification** & **prioritization of activities.**
- Plan is based on **BIA**
- Plan is **simple & easy to understand**.
- Plan is **realistic** in its assumption.
- Sufficient information **backup procedures** for recovery of critical data.
- If **test plan** exist, to what extent it is tested.
- Review **documentation** of actual test.
- **Interview** functional area managers or key employees, do they clearly understand their role.

**Building, Utilities & Transportation**

- Provision for **building engineer** to inspect building & facilities soon after disaster so that damage can be identified & repaired.
- Considered the need of **alternative shelter**, if needed?
- Review **agreements** for use of backup facilities.
- Verify that **backup facilities are adequate & will it be secured**?
- Considered the **failure of electrical power, natural gas, toxic chemical containers, & pipes**?
- Are **building safety features inspected & tested regularly**?

**Information Technology**

- **Analyze** current **IT environment**.
- **Identify prioritized critical applications & systems**.
- **Time requirements** for recovery / availability of critical system included in plan are reasonable or not.
- Arrangements for **emergency telecommunication**.
- **Alternate means of data transmission** if computer network is interrupted & security of such alternate method.
- Is **testing schedule** exist & adequate, date of last test & action taken thereon, if weakness identified.

**Administrative Procedures**

- Does plan cover **administrative & management aspect**.
- Procedures for **disaster declaration**, general **shutdown** & **migration** of operation to backup facility.
- **Duplicate** set of essential **records** & its **retrieval facility** exist in secured location.
- Plan include names & numbers of important **suppliers**.
- Provision or budget for **cost of recovery**.


(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

## BUSINESS PROCESS DESIGN

It means *structuring or restructuring* the *tasks, functionalities & activities for improvising a business system*. It is critical step to understand requirements of the system. It involves (step):

### Present Process Documentation

In this step, *present business process is analyzed & documented*. The key deliverable of this step includes→ well-defined *short-comings of present processes & overall business requirements*.

This step includes following activities:

- Understanding of business & objectives for which it exists;
- Documenting existing business processes; &
- Analysis of the documented processes.

### Proposed Process Documentation

This step is to *design new process requirements* for the system. The design is *based on new system requirements & changes proposed*. The activities include the following:

- Understanding of business processes necessary to achieve business objectives;
- Designing new processes; &
- Documentation of new process, preferably using of CASE tools.

### Implementation of New Process

This step is to implement new / modified processes.

The critical activities includes :

- Validating new process;
- Implementing new process;
- Testing new process.

## SYSTEM DEVELOPMENT

It refers to *process of examining a business situation with the intent of improving it through better procedures & methods*. It has 2 components:

- **System Analysis** is *process of gathering & interpreting facts*, *diagnosing problems*, and *using information to recommend improvements* to the system.
- **System Design** is *process of planning & structuring a new business system* or *one to replace or complement an existing system*.

But before planning, one must thoroughly understand the old system and determine how computers can be used to make its operation more effective.

*(System Design is like blue print for a building, it specifies all features that should be present in the finished product.)*

### Reason for Failure to Achieve System Development Objectives

**1. User Related Issues:**

- **Shifting User Needs:** User requirements for IT are constantly changing. When such changes occur during a development process, development team faces the challenge in developing systems.
- **Resistance to Change:** People generally resist to changes & IS development projects signal changes - often radical - in workplace. When personnel perceive that project will result in personnel cutbacks, threatened personnel will resist & development project may fail.
- **Lack of Users' Participation:** Often users do not participate in development stage because they are preoccupied with their existing work, or do not understand benefits of new system. User apathy 'I have nothing to gain if I participate' is also a reason.
- **Inadequate Testing & User Training:** Often systems are not tested due to lack of time & rush to implement new system. Inadequate user training may be result of poor project planning, lack of training techniques or management not release personnel for training due to operational pressure.

**2. Developer Related Issues**:

- **Lack of Standard Project Management & System Development Methodologies,** it makes difficult to complete projects on time / within budget.
- **Overworked or Under-Trained Development Staff:** In many cases, system developers lack sufficient educational background & requisite skills. Furthermore, in many companies training plan & training budget do not exist.

**3. Management Related Issues:**

- **Lack of Senior Management Support & Involvement:** Developers & users of IS watch senior management to determine 'which systems development projects are important' and act accordingly by shifting their efforts away from any project, which is not receiving management attention.
- **Development of Strategic Systems:** Since strategic decision making is unstructured, the requirements, specifications & objectives for such development projects are difficult to define.

**4. New Technologies:** When org. tries to create a competitive advantage by applying advance technologies, it finds that attaining system development objectives is more difficult because personnel are not familiar with the technology.

### System Development Team

**Steering committee** – Consists of group of key users of IS services, act as a review body for IS plans & applications development. SC ensures that systems development activities satisfy information requirements of managers & users.

**Project management team –** consists of both computer professionals & key users.

**System analysts** determine user requirements, design system, and assist in development & implementation activities.

**Systems designers** – Lead during design, development & implementation stages.

**End-user** – Responsible for system. Generally, end-user seeks guidance from information centre personnel while developing the system.

### Accountants' Involvement in Development Work

An accountant can help in various related aspects:

**1. Return on Investment (ROI):** It defines the return, an entity shall earn on a particular investment i.e. capital expenditure. ROI is a prime consideration for any capital expenditure, entity decides to incur.

ROI analysis requires data like cost of project, expected revenue / benefit etc. This analysis ideally needs to be done before the start of development efforts for better decision making.

For this analysis following data to be generated.

**(a) Cost:** Includes estimates for costs involved in development:

- *Development Costs:* Costs of system development process. E.g. salaries of developers.
- *Operating Costs:* Operating Costs of new system. E.g. hardware / software rental or depreciation charges; salaries of system operators & data processing personnel.
- *Intangible Costs:* It cannot be easily measured. E.g. development of new system may disrupt activities of org. & cause a loss of employee productivity or morale.

**(b) Benefits:** The benefits from developing new or improved IS that can be subdivided into tangible & intangible benefits.

A post implementation analysis is also done to see how system development has benefitted an organization.

E.g. A Company implemented an ERP system at cost of ` 100 crores. Calculated benefits were ` 40 crores p.a. i.e. actual ROI 40% & payback period is around 2.5 years.

**2. Computing Cost of IT Implementation & Cost Benefit Analysis:** For analysis of ROI, accountants need correct costs & returns from the system development efforts. Management shall look Accountant for this purpose.

**3. Skills expected from an Accountant:** Expert in accounting, understand system development efforts, business objectives etc.



(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

**SYSTEMS DEVELOPMENT METHODOLOGY**

A **System Development Methodology** is a *formalized, standardized, well-organized & documented set of activities* used to manage a system development project.
Refers to the *process of examining a business situation with intent of improving it through better procedures & methods.*
A *framework to structure, plan & control the process of developing an IS*. The methodology is characterized by the following:

- **Process –** Project divided into number of identifiable processes, with each process having a starting point & an ending point. Each process comprises several activities, one or more deliverables, and several management control points.
- **Deliverables –** Specific reports & other documentation must be produced periodically during system development.
- **Sign-Offs –** Generally users, managers & auditors provide approvals, often called signoffs. It signify approval of 'development process' and 'system being developed'.
- **Testing** – System must be tested thoroughly prior to implementation to ensure that it meets users' needs as well as requisite functionalities.
- **Training** – A training plan is developed for future users (who will operate & use new system).
- **Controls –** Formal program change controls are established to prevent unauthorized changes to computer programs.
- **Post-implementation Review** of all developed systems must be performed to assess effectiveness & efficiency of new system & of development process.

| WATERFALL MODEL | PROTOTYPING MODEL | INCREMENTAL MODEL | SPIRAL MODEL | RAD MODEL | AGILE MODEL |
|---|---|---|---|---|---|

**WATERFALL MODEL**

This is *a traditional development approach in which each phase or activity is carried in sequence. An activity is undertaken only when the prior step is fully completed*.
These phases include:

- Requirements analysis,
- Specifications & Design Requirements,
- Coding,
- Final Testing,
- Release.

**Characteristics**

- Project is divided into sequential phases.
- Emphasis is on planning, time schedules, target dates, budgets & implementation of an entire system at one time.
- Tight control is maintained by way of written documentation, formal reviews & approval / signoff by user at the end of most phases, before beginning the next phase.

**Strengths:**

- Easy to follow and Ideal for supporting less experienced project teams & project managers.
- Orderly sequence ensures quality, reliability, adequacy & maintainability of developed software.
- Progress of system development is measurable.
- Documentation is produced at every stage, thus allowing people/new team to understand what has been done & what is to be done.

**Weaknesses:**

- Inflexible (not open for change in requirement), slow, costly.
- Project progresses forward, with only slight movement backward.
- Users may not be able to clearly define their requirement at early stages.
- Requirement inconsistencies, missing system components & unexpected development needs are often discovered during design & coding.
- Problems are often not discovered until system testing & may be difficult to correct.
- If requirements change, waterfall model may not work.
- Excessive documentation, whose updation to assure integrity is difficult task & often time-consuming.

**PROTOTYPING MODEL**

The traditional approach takes years to analyze, design & implement a system.
Many times we know a little about the system until & unless we go through its working phases, which are not available. To avoid such issues, organizations use prototyping techniques to develop smaller systems such as DSS, MIS & Expert systems.
*The goal of prototyping approach is to develop a small or pilot version of software called a prototype.*
*A prototype is a usable system or system component that is built quickly & at lesser cost, and with intention of modifying/expanding or even replacing it by a full -scale & fully operational system.*
*As users work with the prototype, they learn about system criticalities & make suggestions.*
*These suggestions are then incorporated to improve the prototype, which is also used & evaluated.*
*Finally, when a prototype is developed that satisfies all user requirements then turned into final system or else it is scrapped.*
*If it is scrapped, knowledge gained from building the prototype is used to develop the real system.*

**Prototyping can be viewed as a series of 4 steps *(Generic phases of Prototyping Model)*:**

- **Identify IS Requirements:** In traditional approach, system requirements are to be identified before the development process starts. However, *under prototype approach, design team needs only fundamental system requirements to build initial prototype, thus it is less formal & less time - consuming.*
- **Develop the Initial Prototype:** *Designers create an initial base model* & give little or no consideration to internal controls, but instead *emphasize on characteristics such as simplicity, flexibility & ease of use.*
- **Test and Revise:** *Designers demonstrate the Initial Prototype to users & give it to them to experiment & ask users to record their likes & dislikes and recommend changes.* Using this feedback, *designers modifies the prototype & resubmits it to users for reevaluation.* This *iterative process of modification & reevaluation continues until the users are satisfied*.
- **Obtain User Signoff of the Approved Prototype:** Users formally approve the final version of prototype & establishes a contractual obligation about what system will & will not, do or provide.


(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

| **Strengths:** | **Weaknesses:** |
|---|---|
| • Improves user participation in system development & communication among project stakeholders.<br>• Resolve unclear objectives; develop & validate user requirements;<br>• Exploit knowledge gained in an early iteration in later iterations.<br>• Identify confusing or difficult functions & missing functionality.<br>• Encourages innovation & flexible designs.<br>• It results in better definition of users' needs & requirements.<br>• Quick implementation of an incomplete, but functional, application.<br>• Errors are detected & eliminated early in developmental process. | • Approval process & control are not strict.<br>• Incomplete or inadequate problem analysis may result in addressing only obvious & superficial needs, & also resulting in current inefficient practices being easily built into the new system.<br>• Requirements may frequently change significantly.<br>• Designers may prototype too quickly, without sufficient upfront user needs analysis, resulting in an inflexible design that limits future system potential.<br>• Prototyping can be successful only if users devote significant time in experimenting & provide suggestions.<br>• Sometimes, System Developers minimize the testing & documentation process of approved IS which can make the approved system error-prone & difficult to maintain.<br>• Dissatisfaction of users if system developers are unable to meet all user demands for improvements<br>• Impatience by users when they have to go through too many interactions of the prototype. |

| **INCREMENTAL MODEL** | **Strengths:** | **Weaknesses:** |
|---|---|---|
| *It is a method of software development where model is designed, implemented & tested incrementally (a little more is added each time) until the product satisfies all of its requirements. It combines the elements of waterfall model with iterative philosophy of prototyping.*<br>The product is decomposed into a number of components, each of which are designed & built separately (termed as builds).<br>Each component is delivered to client when it is complete.<br>A series of mini-waterfalls are performed on each components (builds) before proceeding to next increment, followed by iterative Prototyping. | • Exploit knowledge gained in early increment in later increments.<br>• Moderate control is maintained over the life of project by way of written documentation, formal review & approval/signoff by user at designated milestones.<br>• Concrete evidence of project status can be obtained.<br>• More flexible & less costly to change scope & requirements.<br>• Mitigate integration & architectural risks at earlier stage.<br>• Gradual implementation provides ability to monitor the effects of incremental changes & to make adjustments before organization is negatively impacted.<br>• Customer can respond to features & review the product for needful change. | • Since it uses a series of mini-waterfalls approach for a small part of the system before moving onto next increment, thus its lack overall consideration for overall system.<br>• Each phase of an iteration is rigid & do not overlap each other.<br>• Since all requirements are not gathered upfront for entire life cycle, thus problems may arise pertaining to system architecture.<br>• Some modules are completed much earlier than others, thus well-defined interfaces are required. |

| **SPIRAL MODEL** | **Strengths:** | **Weaknesses:** |
|---|---|---|
| *It combines features of prototyping model & waterfall model. There are specific activities which are done in one iteration (spiral) where the output is a small prototype of the large software. The same activities are repeated for all the spirals till the entire system is built. It is intended for large, expensive & complicated projects. Game development is a main area where this model is used & needed, because of size & constantly shifting goals of those large projects.*<br>**Characteristic:**<br>• *New system requirements* are *defined in as much detail* as possible. E.g. By interviewing.<br>• A *preliminary design* is created for the new system. This phase is most important part of "Spiral Model" in which all possible alternatives are analyzed & strategies are decided, for using them in identifying & resolving all possible risks in project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to deal with potential changes in the requirements.<br>• A *first prototype* of new system is constructed from preliminary design.<br>• A *second prototype* is evolved by evaluating the first prototype. | • Enhances risk avoidance.<br>• Useful in helping for optimal development of a given software with iteration based on project risk.<br>• Can incorporate Waterfall, Prototyping & Incremental methodologies.<br>• Provide guidance as to which combination of these models (Waterfall, Prototyping & Incremental Model) best fits a given software iteration, based upon type of project risk.<br>• Additional functionality can be added later. | • Challenging to determine exact composition of development methodologies for each iteration.<br>• May prove highly customized to each project, & thus limits its reusability & make it complex.<br>• Skilled & Experienced project manager is required to apply it to any given project.<br>• No established controls exist for moving from one cycle to another cycle which can generate more work for next cycle.<br>• No firm deadlines, cycles continue with no clear termination condition leading to inherent risk of not meeting budget or schedule. |


(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

| RAPID APPLICATION DEVELOPMENT (RAD) MODEL | Strengths: | Weaknesses: |
|---|---|---|
| This methodology *uses minimal planning in favor of rapid prototyping. Planning of software developed using RAD is interleaved with writing software itself* (i.e. process of writing the s/w itself involves the planning required for developing the product). *The lack of extensive pre-planning allows software to be written much faster & makes it easier to change requirements*.<br>Key objective is fast development & delivery of high quality system at low cost,<br>Key emphasis is on fulfilling business needs, while technological or engineering excellence is of lesser importance.<br>If project starts to slip, emphasis is given on reducing requirements to fit it in timebox, not in increasing deadline. | • Operational version of an application is available much earlier than with Waterfall, Incremental or Spiral.<br>• Produce system more quickly & at lower cost.<br>• Quick initial reviews are possible.<br>• Concentrates on essential system elements from user viewpoint.<br>• Provides ability to rapidly change system design as demanded by users.<br>• Leads to tighter fit b/w user requirements & system specifications. | • Fast speed & lower cost may affect adversely the system quality.<br>• Project may end up with more requirements than needed (gold-plating).<br>• May lead to inconsistent designs within & across systems.<br>• May violate programming standards related to inconsistent documentation,<br>• Lack of attention to future system administration needs built into system.<br>• Some modules are completed much earlier than others, well–defined interfaces are required. |

| AGILE MODEL | Strengths: | Weaknesses: |
|---|---|---|
| It is software development methodologies *based on iterative & incremental development, where requirements & solutions evolve through collaboration between self-organizing, cross-functional teams.*<br>*It promotes adaptive planning, evolutionary development & delivery; time boxed iterative approach and encourages rapid & flexible response to change.*<br>*It is framework that promotes foreseen interactions throughout the development life cycle.*<br>**Key features of Agile Model:**<br>• Customer satisfaction by rapid delivery of useful software;<br>• Changing can be done, even in later phases of development;<br>• Working software is delivered faster (in weeks rather than months);<br>• Sustainable development helps to maintain a constant pace;<br>• Close, daily co-operation b/w business people & developers;<br>• Projects are built around trusted & motivated individuals;<br>• Continuous attention to technical excellence & good design. | • Enables to respond to changing requirements.<br>• Face to face communication & continuous inputs from customer representative leaves a little space for guesswork.<br>• Documentation is crisp & to the point to save time.<br>• It satisfy customers by delivering high quality software in least possible time. | • Difficult to assess the efforts required at beginning of SDLC.<br>• Lack of emphasis on necessary designing & documentation.<br>• Team focuses on verbal communication rather than on documents or manuals which leads to potential threats to business continuity & knowledge transfer.<br>• Requires more re-work due to lack of long-term planning, or when various components of software are combined & forced to interact.<br>• Project can easily get off track if the user is not clear about the final outcome. |

## SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

The system development process is initiated when it is realized that a particular business process of org. needs computerization or improvement.

SDLC consists of a generic sequence of steps or phases in which each phases of SDLC uses the results of previous one and provides system designers & developers to follow a sequence of activities.

I. Preliminary Investigation
II. Systems Requirement Analysis
III. Systems Design
IV. Systems Acquisition
V. Systems Development
VI. Systems Testing
VII. Systems Implementation
VIII. Post Implementation Review & Maintenance

**Possible advantages of SDLC from the perspective of IS Audit**

- IS Auditor can have clear understanding of various phases of SDLC on the basis of detailed documentation created during each phase of SDLC.
- On the basis of his/her examination, can state in his/her report about compliance with procedures, if any, set by management.
- IS Auditor with his technical knowledge & skills can guide during various phases of SDLC.
- IS Auditor can provide an evaluation of the methods & techniques used through various phases of SDLC.


(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

**PRELIMINARY INVESTIGATION – A preliminary investigation is normally initiated by some sort of system request.**

*When user comes across a problem in the existing system or a totally new requirement for computerization, a formal request has to be submitted for system development.*

Its aim is *to determine & analyze the strategic benefits in implementing the system* through evaluation & quantification of - productivity gains; future cost avoidance; cost savings, and Intangible benefits like improvement in morale of employees. The *deliverable of preliminary investigation phase includes a report including feasibility study observations*.

**Identification of Problem:** *Define the problem clearly & precisely, after critical study of existing system & several rounds of discussions with user group.*

Managers & users may submit a request for new system to IS department. If need seems genuine, a system analyst is assigned to perform preliminary investigation who submits all proposals to steering committee for evaluation & to identify those projects that are most beneficial to org. Purpose of preliminary investigation is to evaluate the project request feasibility.

**Identification of Objectives:** After identification of problem, *work out & precisely specify the objectives of proposed solution*. (E.g. In Railways: Introduce system, to book ticket faster.)

**Delineation of Scope:** *Defines its typical boundaries that clearly & comprehensibly states to user management the extent and defines 'what will be addressed by the solution & what will not'.* Often, scope becomes a contentious issue b/w development & user organizations. Hence, outlining scope in beginning is essential. In determining scope consider following dimensions:

**Functionality Requirements:** What functionalities will be delivered through solution?

**Data to be Processed:** What data is required to achieve these functionalities?

**Control Requirements:** What are control requirements for this application?

**Performance Requirements:** What level of response time & execution time is required?

**Constraints:** What are conditions that input data has to conform to?
E.g. No. of characters.

**Interfaces:** Is there any special hardware/software that application has to interface with?
E.g. Payroll application have to interface with attendance monitoring system already installed.

**Reliability requirements:** It is measured by its ability to remain uncorrupted in during inadvertent / deliberate misuse & probability of failure-free operations.

**Aspects needs to be kept in mind while eliciting information to delineate scope:**

- Different users represent problem & required solution in different ways. So system developer should take the need from initiator of project as the basis of scope.
- Initiator of project may be from senior management & actual users may be from operating levels. Understanding their profile helps in designing appropriate user interface.
- While presenting proposed solution for a problem, development org. has to clearly quantify the economic benefits to user org.
- Understand the impact of solution on org. Solutions with wider impact needs greater resistance. E.g. on ERP implementation, if not able to handle it may have disastrous consequences.
- Beside economic benefits, other factors are to be considered from the perspective of user management & same should be resolved. E.g. In a security system, how foolproof it is.

**2 methods for analysis of scope of project in SDLC:**

- **Review Internal Documents:** Analysts conducting investigation, first try to learn about org. by examining org. charts & studying written operating procedures.
- **Conduct Interviews:** Written documents tell how systems should operate, but not about requirements of systems proposed & users' views about current operations. To learn these details, analysts should conduct interviews, which allow analysts to know more about requirement of project.

**Feasibility Study:** *After possible solution options are identified, project feasibility i.e. likelihood that proposed system will be useful for org. is determined.* Feasibility study refers to process of evaluating alternative systems through cost/benefit analysis, by system analyst, so that most feasible & desirable system can be selected for development. It comprises:

- **Technical Feasibility** *(Is technology needed available?)***:** It answers whether proposed system is feasible with existing or expected computer hardware & software technology. The technical issues includes:
  - *Does necessary technology exist to do what is suggested (& can it be acquired)?*
  - *Does proposed equipment have technical capacity to hold data required to run new system?*
  - *Can proposed application be implemented with existing technology?*
  - *Will proposed system provide adequate responses to inquiries, regardless of number or location of users?*
  - *Can system be expanded if developed?*
  - *Are there technical guarantee of accuracy, reliability, ease of access & data security?*
- **Financial Feasibility** *(Is system viable financially?)***:** It checks whether proposed system may be costly for user organization.
- **Economic Feasibility** *(Evaluation of Return on Investment?)***:** It includes an evaluation of incremental costs & benefits expected if proposed system is implemented. It includes estimating:
  - *Cost of conducting a full systems investigation;*
  - *Cost of hardware & software for the class of applications being considered;*
  - *Benefits in form of reduced costs or fewer costly errors; and*
  - *Cost if nothing changes (i.e. if proposed system is not developed).*
- **Schedule or Time Feasibility** *(Can system be delivered on time?)***:** It involves estimation of time it will take a new or revised system to become operational.
- **Resources Feasibility** *(Are human resources reluctant for system?)***:** This focuses on human resources. Implementing sophisticated software solutions not suitable for locations which lack skilled personnel.
- **Operational Feasibility** *(How will system work?)***:** It is concerned with finding views of workers, employees, customers & suppliers about the use of new system. A system can be highly feasible in all respects except the operational and fails miserably because of human problems. Questions which help in testing operational feasibility:
  - *Is there sufficient support for the system from management & from users?*
  - *Are current business methods acceptable to users?*
  - *Have the users been involved in planning & development of project?*
  - *Will proposed system cause harm? Will it produce poorer results?*
  - *Will loss of control result in any areas? Will accessibility of information be lost?*
  - *Will individual performance be poorer after implementation than before?*
- **Behavioral Feasibility** *(Is system going to bring any adverse effect on quality of work life?)***:** If data input for system is not readily available or collectable, then system may fail.
- **Legal Feasibility** *(Is system valid in legal terms?)***:** Any system, which violate the local legal requirements should be rejected.



(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

**Reporting Results to Management:** *Provides one or more solution alternatives and estimates the cost & benefits of each alternative and reports these results to management.* From analyst's report, management should determine what to do next. Not all projects submitted for evaluation & review may get accepted.

**Internal Control Aspects:** Management is responsible for implementing IC to ensure business objectives. *During system developments, controls should be placed well as it is difficult to place controls post development.* For validating IC, entity may have an internal audit team or may engage outside experts for the same. key control queries may include:

- Whether problem is defined properly?
- Whether feasibility studies have been done properly?
- Whether results of feasibility studies have been documented?
- Whether management report submitted reflects outcome of feasibility studies?

**SYSTEM REQUIREMENTS ANALYSIS – Major deliverable is Systems Requirements Specification (SRS).**

*This phase includes a thorough & detailed understanding of current system, identify the areas that need modification to solve the problem and determine user/managerial requirements.*

Objective to generate SRS or Objective of System Requirements Analysis Phase:

- Identify & consult stake owners to determine their expectations & resolve their conflicts;
- Analyze requirements to detect & correct conflicts & determine priorities;
- Gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation;
- Verify that requirements are complete, consistent, unambiguous, verifiable, modifiable, testable & traceable;
- To model activities e.g. developing models to document Data Flow Diagrams, E-R Diagrams.

**Fact Finding:** Every system is built to meet some set of needs.
E.g. of needs - lower operational costs, better information to managers, smooth operations for users or better levels of services to customers.

*Fact-finding techniques / tools to assess these needs:* ----------→

***Documents*:** Document like procedure manuals, input forms, output forms, diagrams of how current system works, hierarchy of users & manager responsibilities, job descriptions, program codes associated with the current system, etc. are collected & analyzed for understanding user needs & current system.
***Questionnaires*:** Users & managers are asked to complete questionnaire about the problem of existing system & requirements of new system. It collects large data quickly. It should be skillfully drafted for quick response.
***Interviews*:** Users & managers are interviewed to extract information in depth.
***Observation*:** Analyst personally visit work place & observe their (users) working.

**Analysis of Present System: (Investigation of Present IS)**
It involves *collecting, organizing & evaluating facts about system & environment in which it operates*.
Enough information should be assembled so that a qualified person can understand present system without visiting any of operating departments.
*Review of existing methods, procedures, data flow, outputs, files, input & internal controls should be intensive to fully understand the present system & its related problems.*
The following areas should be studied in depth: ----------→

- **Reviewing Historical Aspects:** System analyst should investigate 'what system changes have occurred in past including operations' that have been successful or unsuccessful with computer equipment & techniques.
- **Analyzing Inputs:** System analyst should know various sources to input data. He must understand nature of each form, 'it's contained', 'who prepared it', 'its initiation, completion & distribution', etc. It will enable him/her to determine how these inputs fit into framework of present system.
- **Reviewing Data Files:** Analyst should investigate the data files maintained by each department, their number, size, locations, users & frequency of their usage. He should also review all on-line & off-line files. He should also consider common data files & their size.
- **Reviewing Methods, Procedures & Data Communications:** Methods & procedures transform input data into useful output. Method is way of doing something; Procedure is a series of logical steps by which a job is accomplished. A procedure review is an intensive survey of the methods by which each job is accomplished. Its basic objective is to eliminate unnecessary tasks or to improve present IS. System analyst also needs to review & understand the present data communications used by organization.
- **Analyzing Outputs:** Analyst should examine outputs or reports to determine 'how well it meets organization's needs. He should understand what information is needed & why, who needs it & when & where it is needed. Often, many reports are carry-over from earlier days & have little relevance to current operations. Attempts should be made to eliminate all such reports in the new system.
- **Reviewing Internal Controls:** Examination of present system of IC may indicate weaknesses that should be removed in the new system.
- **Modeling (Documenting) the Existing System:** After analyzing the present system in terms of inputs, methods, procedures, output, internal controls, etc. it must be properly documented. Flow charts helps to disclose gaps & duplication in data gathered. It also allows a thorough understanding of numerous details & related problems in the present operation.
- **Undertaking Overall Analysis of Existing system:** Analyst undertake overall analysis of present system in terms of present workload; current personnel requirements; present costs-benefits.

**Analysis of Proposed Systems:** After thorough analysis of present IS and considering strengths & short comings of present system, proposed system specifications must be clearly defined, in conformity with project's objectives set forth at the first stage, in terms of following:

- Outputs of proposed system.
- Input & source of input data.
- Methods & procedures for conversion of input into output.
- Workload & Internal control of proposed system.
- Databases with desired capabilities e.g. online processing capabilities.

**System Development Tools:** Many tools & techniques have been developed to improve Current IS & to Develop New Ones. These are used:

- To conceptualize, clarify, document & communicate the activities & resources involved in org. & its IS;
- To analyze present business operations, management decision making & information processing activities;
- To propose & design new or improved IS to solve business problems or pursue business opportunities.


(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

Major tools used for system development: (4 categories)

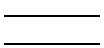
| **System Components & Flows:** These tools documents the data flow among major resources & activities of an IS.<br>- Flowchart - Data Flow Diagram - Risk Matrix | **User Interface:** Designing interface b/w end users & computer system is a major consideration of a system analyst while designing new system.<br>- User Interface Layout & Forms | **Data Attributes & Relationship:** Data resources in IS are defined, catalogued and designed by this category of tools.<br>- Data Dictionary | **Detailed System Processes:** These tools helps the programmer to develop detailed procedures & processes required in design of computer program.<br>- Decision Table - Decision Tree | **Others:**<br>- Structured English<br>- CASE Tools |
|---|---|---|---|---|

- **Flowcharts:** Pictorial representation technique used by analysts to represent the inputs, outputs & processes of a business process and algorithm or process showing the steps through various boxes connecting with arrow.
- **Data Flow Diagrams:** It uses few simple symbols to illustrate the flow of data among external entities (e.g. people or organizations), processing activities & data storage elements.

 Data Sources & destinations — People & organizations that send & receive data.

 Data flows — Flow of data into or out of a process.

 Transformation process — Processes that transform data from inputs to outputs.

 Data stores — Storage of data.

- **System Components Matrix:** It provides a matrix framework to document the resources used, activities performed & information produced by an IS and highlights how basic activities of input, processing, output, storage & controls are accomplished in an IS.
- **User Interface Layout and Forms:** Several type layout forms for both soft & hard copy are used to model input/output components of IS. Types of layout & forms:
  - **Layout form & Screen Generator:** These are for printed report used to format or "paint" the desired layouts and contact without having to enter complex formatting information.
  - **Menu Generator:** It outlines the functions, which the system is aimed to accomplish. Menu may be linked to other submenus.
  - **Report Generator:** It perform similar functions as in screen generators. It also indicate totals, paging, sequencing & control breaks in creating samples of desired report.
  - **Code Generator:** It allows analyst to generate modular units of source code from the high level specifications provided by system analyst.
- **Data Dictionary:** A data dictionary is a computer file about data. Each computer record of a data dictionary contains information about a single data item (in detailed- name, size, type, files & program using these data, individual users permitted to access, name of computer program that modify, etc.) used in business IS.
- **Decision Table:** It is a table accompanying a flowchart, defining possible contingencies that may be considered within program & appropriate course of action for each contingency.
  The 4 parts of decision table: ○ Condition Stub ○ Action Stub ○ Condition Entries ○ Action Entries
- **Decision Tree:** Decision Tree or tree diagram is a support tool that uses a tree-like graph or model or structure of decisions & their possible consequences.
- **Structured English:** It is also known as Program Design Language (PDL), is the use of English language with syntax of structured programming.
- **CASE Tools:** CASE refers to automation of anything that humans do to develop systems. Data flow diagram & flow charts are commonly generated by systems developers using the on-screen drawing modules found in CASE (Computer-Aided-Software Engineering) software packages.

**Systems Specification:** At the end of analysis phase, the systems analyst prepares a document called **Systems Requirement Specifications (SRS)**. SRS contains following:

- **Introduction:** Goals, Objectives, Scope & Environment of computer-based system.
- **Information Description:** Problem description; Information content, flow & structure of existing IS.
- **Functional Description:** Diagrammatic representation of functions & their processing.
- **Behavioral Description:** Response to external events & internal controls.
- **Validation Criteria:** To validate functions, performance & constraints.
- **Appendices:** Data flow Diagrams; Tabular Data; Algorithms charts, graphs, etc.
- **SRS Review:** Hands over the SRS document to user or customer for review. User should sign after ensuring that SRS document represents existing processes accurately. Then it becomes contract b/w users & development org.

**Roles Involved in SDLC:** A variety of tasks during SDLC are performed by special teams/committees/individuals based on requisite expertise & skills. Some generic roles are described:

- **Steering Committee:** Provide overall directions, review progress of project, undertake corrective actions like rescheduling, re-staffing etc.
- **Project Manager:** Responsible for more than one project, deals with client, delivering the project within time/budget & periodically reviews progress, etc.
- **Project Leader:** Project leader is dedicated to a project, who ensure its completion & fulfillment of objectives, reviews project status more frequently than Project Manager & entire project team reports to him/her.
- **Systems Analyst / Business Analyst:** Conduct interviews with users & understand their requirements. S/he is a link b/w users & designers/programmers, who convert users' requirements into system requirements and plays a critical role in Requirements analysis & Design phase.
- **Module Leader/Team Leader:** A project is divided into several modules and development responsibility for each module is assigned to Module Leaders, they are responsible for delivering tested modules within stipulated time & cost.
- **Programmer/Developers:** Converts design into programs by coding, using programming language.
- **Database Administrator:** DBA handles multiple projects, ensures integrity & security of information stored in database and also helps in database performance issues. Inclusion of new data elements is done only with the approval of DBA.
- **Quality Assurance:** This team sets the standards for development & checks compliance with these standards by project teams on a periodic basis.
- **Testers:** Testers are junior level quality assurance personnel who test programs & subprograms as per plan given by module / project leaders & prepare test reports.
- **Domain Specialist:** Whenever a project team develops an application in a field that's new to them, they take the help of domain specialist. E.g. If team undertakes application development in Insurance, Insurance expert will assist them at different stages.
- **IS Auditor:** S/he should be involved at Design Phase & final Testing Phase to ensure existence & operations of the Controls in new software.

**Internal Controls:** This includes:

- Whether present system analysis has been properly done?
- Whether appropriate domain expert was engaged?
- Whether all user requirements of proposed system have been considered?
- Whether SRS document has been properly made and reviewed?



(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

**SYSTEM DESIGN – Design phase documents include a 'blueprint' for design with necessary specifications for hardware, software, people & data resources.**
*The objective is to design an IS that best satisfies the users/managerial requirements. It describes the parts of system & their interaction; sets out how system shall be implemented using chosen hardware, software & network facilities; specifies the program and the database specifications and the security plans and further specifies the change control mechanism to prevent uncontrolled entry of new requirements.* Once the detailed design is completed, the design is then distributed to system developers for coding.

**(a)** **Architectural Design:** This deals with the organization of applications in terms of hierarchy of modules & sub-modules wherein major modules; functions & scope of each module; interface features of each module; modules that each module can call directly or indirectly & Data received from / sent to / modified in other modules are identified.

**(b)** **Design of Data/Information flow:** This includes designing the data/information flow for the proposed system, the inputs (for designing) that are required are - existing data / information flows, problems with the present system, and objective of the new system. (All these have been documented in SRS in Analysis Phase)

**(c)** **Design of Database:** This involves determining its scope ranging from local to global structure. The design of database involves 4 major activities.

| Conceptual Modeling | Data Modeling | Storage Structure Design | Physical Layout Design |
|---|---|---|---|
| These describe the application domain via entities/objects, attributes of these entities/objects and static & dynamic constraints on these entities/objects, their attributes, and their relationships. | Conceptual Model need to be translated into data model so that they can be accessed & manipulated by both high-level & low-level programming languages. | Decisions must be made on how to linearize & partition the data structure so that it can be stored on some device. | Decisions must be made on how to distribute the storage structure across specific storage media & locations & the computers in a LAN or WAN. |

**(d)** **User Interface Design:** It involves determining the ways in which users will interact with a system.

**Important factors to be considered by system analyst while designing user input/ output forms.**

| Characteristic | Input Design | Output Design |
|---|---|---|
| **Content:** Actual pieces of data to be gathered to produce the required output to be provided to users. | Analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. New documents for collecting such information may be designed. | Contents of a weekly output report to sales manager might consist of sales person's name, amount of each product sold by each salesperson to each major client category. |
| **Timeliness:** When users need outputs, say on regular, periodic basis - daily, weekly, monthly, quarterly or annually. | Data needs to be inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, plan must be established regarding when inputs will be entered. | A sales manager may require weekly sales report. Other users, such as airline agents require real- time information to render better client service. |
| **Format:** Input format refers to the way data are physically arranged. Output format refers to the arrangement referring to data output on a printed report or in a display screen. | Once data contents & media requirements are determined, input formats are designed with few constraints like - type & length of each data field & any other special characteristics (number of decimal places etc.). | Format of information reports should be so devised that it assists in decision-making, identifying & solving problems, planning & initiating corrective action and searching. |
| **Media:** Input-output medium refers to the physical device used for input, storage or output. | Choose suitable input media & devices on which to enter the data. E.g. magnetic tapes, magnetic disks, key- boards, optical character recognition, pen- based computers & voice input etc. | Several output media are available. E.g. video display, paper, microfilm, magnetic tape/disk and voice output. |
| **Form:** Form refers to the way information is inputted in input form & content is presented to users in various output forms text, graphics, video & audio. | Forms are pre- printed papers that require people to fill in response in a standardized way. Forms capture information & often will be input to the computer. Forms often serve as source documents for data entry personnel. | Form of output should be designed keeping in view the requirements of the concerned user. |
| **Input Volume/ Output Volume:** Input volume refers to amount of data that must be entered in computer system at any one time. The amount of data output required at any one time is known as output volume. | In some DSS & many real-time processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy. | Use high-speed printer or rapid-retrieval display unit, which are fast & frequently used output devices in case volume is heavy. |

**(e)** **Physical Design:** Concentrates on the issues like the type of hardware for client & server application, Operating systems to be used, type of networking, periodical batch processing, online or real-time processing, frequency of input/output, etc.

**(f)** **System's Operating Platform:** In some cases, the new system requires an operating platform including hardware, network & system software not currently available in org. E.g. – a DSS might require high-quality graphics output not supported by existing hardware & software. The new hardware/system software platform required to support the application system will then have to be designed for requisite provisions.

**(g)** **Internal Design Controls:** This include

- Whether management reports of stage I & II, were referred by System Designer?
- Whether all control aspects have been properly covered?
- Whether controls put in place in system, appear in documentation done at this stage?
- Whether a separate review of design document has been done by internal auditor?


(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

**SYSTEM ACQUISITION**

After a system is designed either partially or fully, the next phase of SDLC starts, which relates to acquisition of operating infrastructure including hardware, software & services.

**(a) Acquisition Standards:** Management should establish acquisition standards that address the security & reliability issues in development of software.
Acquisition standards should focus on following:

- Ensuring *security, reliability & functionality* already built into a product;
- Ensuring *managers reviews vendor contract & licensing* and *acquiring products compatible with existing systems*;
- *Invitations-to-tender soliciting bids from vendors* when acquiring hardware or integrated systems of hardware & software;
- *Request-for-proposals soliciting bids when acquiring third-party developed software*; and
- Establishing acquisition standards to ensure *functional, security & operational requirements to be accurately identified and clearly detailed in RFP*.

**(b) Acquiring Systems Components from Vendors:** At the end of design phase, org. gets a reasonable idea of types of hardware, software & services; it needs for the system being developed. Management also decides whether the hardware is to be purchased, leased or to be rented. Then RFP from vendors is called. For acquisition of H/w & S/w consider:

- **Vendor Selection:** Vendor selection is done prior to sending RFP & RFP are sent only to selected vendors. For this, consider *background & location advantage* of vendor, *financial stability* of vendor, *market feedback* of vendor performance, *in terms of price, services etc.*
- **Geographical Location of Vendor:** Look whether the *vendor has local support service centres or persons*.
- **Presentation by Selected Vendors:** All vendors, whose proposals are accepted, are allowed to make presentation. *Evaluates vendor's proposals*.
- **Evaluation of Users Feedback:** Analyze the feedback from present users.

**(c) Other Acquisition Aspects and Practices:** In addition to above, there are several other acquisition aspects:

**(i) Hardware Acquisition:** In procuring hardware, management depends upon vendor for support services, systems design, education & training etc., and expansion of computer installation is continuous process; therefore, this is not just buying the hardware & paying vendor for it but it amounts to an enduring alliance with supplier.

**(ii) Software Acquisition:** Once user requirements are identified in terms of input & output, the application system requirement must be assessed by system analyst. This helps the system developers in deciding about the nature of the systems software & computer hardware that will be most suitable for every situation. At this stage, system developers must determine whether the application software should be created in-house or acquired from a vendor.

**(iii) Contracts, Software Licenses and Copyright Violations:**
Contracts between an organization & a software vendor should clearly describe the rights & responsibilities of the parties to the contract, and contracts should be in writing.
Software license grants permission to use computer software.
Copyright laws protect proprietary as well as open-source software. The use of unlicensed software or violations of a licensing agreement expose org. to possible litigation.

**(iv) Validation of Vendors' proposals:** It involves *evaluating & ranking the proposals submitted by vendors*. This process is quite difficult, expensive & time consuming (but still to be done). The following factors to be considered:

- *Performance capability* of each proposed System *in Relation to its Costs*;
- *Costs & Benefits* of each proposed system;
- *Maintainability* of each proposed system;
- *Compatibility* of each proposed system *with Existing Systems*; and
- *Vendor Support.*

**(v) Methods of Validating the proposal:**

- **Checklists:** The various criteria are put in check list in the form of suitable questions against which the responses of various vendors are validated.
- **Point-Scoring Analysis:** In this, first assign a point/score (say 1 to 10) for each evaluation criteria based on its importance. Then, award points/score (say 7 out of 10) to each vendor after considering their responses. The points/score are added & the vendor's proposal with the highest point/score will be selected.
- **Public Evaluation Reports:** Several independent agencies compare and differentiate the hardware & software performance for various manufacturers & publish their reports. These reports can be referred to identify a suitable vendor.
- **Benchmarking Problems related Vendor's Solutions:** Testing whether a solution offered by the vendor meets the requirements of the job on hand of the buyer.
- **Testing Problems:** Test problems are devised to test the true capabilities of the hardware, software or system. E.g. Test problems developed to evaluate response time for 2 or more jobs in multi-tasking environment.


(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

**SYSTEM DEVELOPMENT:**

This phase is supposed to *convert the design specifications into a functional system under the planned operating system environments. Application programs are written, tested & documented, conduct system testing. Finally it results into a fully functional & documented system.*

Characteristics of a good coded application & programs:

- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters & hard coding of some data could result in failure of program after some time.
- **Robustness:** It refers to the applications' strength to uphold its operations in adverse situations by taking into account all possible inputs & outputs of a program in case of least likely situations.
- **Accuracy:** It refers not only to 'what program is supposed to do', but should also take care of 'what it should not do'.
- **Efficiency:** It refers to performance per unit which should not be unduly affected with increase in input values.
- **Usability:** It refers to a user-friendly interface & easy-to-understand internal/external documentation.
- **Maintainability:** It refers to the ease of maintenance of program even in absence of program developer.

Other related aspects of this phase are given as follows:

- **Program Coding Standards:** The logic of program outlined in flowcharts is converted into program statements or instructions at this stage. Different programmers may write a program using different sets of instructions but each giving the same results. Therefore, coding standards are defined, which provide simplicity, interoperability, compatibility, efficient utilization of resources & least processing time.
- **Programming Language:** Application programs are coded in the form of statements or instructions & the same is converted by compiler to object code for the computer to understand & execute. E.g. C++, JAVA, C#, JavaScript.
- **Program Debugging:** Debugging refers to correcting programming language syntax & diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from source code written by programmer into machine language instructions.

  Debugging can be boring task: (4 Steps)
  1. Inputting source program to compiler,
  2. Letting compiler to find errors in program,
  3. Correcting erroneous line of code, and
  4. Resubmitting corrected source program as input to compiler.
- **Testing the Programs:** A careful & thorough testing of each program is imperative to successful installation of any system. The programmer should plan the testing to be performed, including testing of all possible exceptions.
- **Program Documentation:** Writing narrative procedures & instructions for people, who will use software throughout program life cycle. Users should carefully review documentation to ensure that software behave as documentation indicates. If they do not, documentation should be revised. Documentation should be prepared in such a way that user can clearly understand instructions.
- **Program Maintenance:** The requirements of data processing applications are subject to periodic change. This calls for modification of various programs. There are separate categories of programmers called maintenance programmers, who are entrusted with this task.

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

## SYSTEM TESTING

Testing is a process used to identify correctness, completeness & quality of developed computer software. Testing uncover errors in a minimum amount of time & efforts. However, testing cannot show the absence of defect, it can only show that software defects are present. Different levels/facets of Testing:

**Unit Testing:** A unit is the smallest testable part of an application, which may be an individual program, function, procedure, etc. Unit testing is a software verification & validation method in which a programmer tests if individual units of source code are fit for use. The 5 categories of tests that a programmer typically performs on a program unit:

- **Functional Tests:** It checks 'whether programs do, what they are supposed to do or not'. By inputting values, programmer checks whether actual result & expected result match.
- **Performance Tests:** It verify the response time, execution time, primary & secondary memory utilization & traffic rates on data channels & communication links.
- **Stress Tests:** It determine the stability of system or entity. It involves testing beyond normal operational capacity, often to a breaking point, to observe the results. It is designed to overload a program in various ways to determine the limitations of the program.
- **Structural Tests:** It is concerned with examining the internal processing logic of a software system. E.g. if a function calculate tax, verification of its logic is a structural test.
- **Parallel Tests:** Same test data is used in the new & old system and output results are then compared.

In terms of techniques, Unit Testing is classified as Static Analysis Testing and Dynamic Analysis Testing.

**Static Analysis Testing:** It is normally conducted on source programs & do not normally require executions in operating conditions. It includes:

- **Desk Check:** This is done by the *programmer him/herself*. S/he checks for logical syntax errors & deviation from coding standards.
- **Structured Walk Through:** The *application developer leads other programmers* to scan through the text of program & explanation *to uncover errors*.
- **Code Inspection:** The program is *reviewed by a formal committee* with formal checklists.

**Dynamic Analysis Testing:** It is normally conducted through execution of programs in operating conditions. It includes:

- **Black Box Testing:** It takes an external perspective of the test object. In this, test designer selects typical inputs (simple, extreme, valid & invalid input) and executes to uncover errors. He has no prior knowledge of test object's internal structure.
- **White Box Testing:** It uses an internal perspective of system to design test cases based on internal structure. It requires programming skills to identify all paths through software.
- **Gray Box Testing:** It uses combination of black box testing & white box testing.

**Integration Testing:** It is an activity of software testing in which individual software modules are combined & tested as a group. It occurs after unit testing & before system testing.

It is carried out in 2 manners:

- **Bottom-up Integration:** It is traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub- system testing, and then testing of the entire system.
- **Top-down Integration:** It starts with the main routine, and stubs are substituted, for the modules directly subordinate to main module. Once the main module testing is complete, stubs are substituted with real modules one by one, and these modules are tested with stubs. This process continues till the atomic modules are reached.

**Regression Testing:** Each time a new module is added or any modification made in the software, it changes. New data flow paths are established, new I/O may occur & new control logic is invoked.

These changes may cause problems with functions that previously worked flawlessly.

In the context of integration testing, regression tests ensure that changes or corrections have not introduced new faults.

Data used for the regression tests should be same as the data used in the original test.

**System Testing:** It is a process in which software & other system elements are tested as a complete system. It is conducted when software as a whole is operational. The purpose of system testing is to ensure that the new or modified system functions properly. These test procedures are often performed in a non-production test environment. It includes:

- **Recovery Testing:** Testing 'how well the application is able to recover from crashes, hardware failures & other similar problems'.
- **Security Testing:** Determining whether an IS protects data & maintains functionality as intended or not. It cover CIA.
- **Stress or Volume Testing:** Determining the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, to observe results.
- **Performance Testing:** Determining the speed or effectiveness of a computer, network, software program or device. It compares the new system's performance with similar systems using well defined benchmarks.

**Final Acceptance Testing:** It is conducted when the system is ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards & satisfies the users.

It has 2 major parts:

- **Quality Assurance Testing:** It ensures that new system satisfies the prescribed quality standards & development process is as per organization's quality assurance policy. (By Developer Org.)
- **User Acceptance Testing:** It ensures that the functional aspects expected by users have been well addressed in new system. (By User Org.)
  There are 2 types of user acceptance testing:
  - **Alpha Testing:** This is the first stage, often performed by users within organization. (With his own)
  - **Beta Testing:** This is the second stage, performed by external users (By Certified User), during real life execution of the project. It normally involves sending the product outside development environment for real world exposure & receives feedback for analysis & modifications.



(rajveer.an.indian@gmail.com)

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

**SYSTEM IMPLEMENTATION** *(Replacing Existing system Or Major Modification in Existing System)*

The process of ensuring that IS is operational & then allowing users to take over its operation for use & evaluation is called Systems Implementation. Implementation includes all those activities that take place to convert from old system to new.

Generic key activities involved in System Implementation include: ----------→

- Conversion of data to the new system files;
- Training of end users;
- Completion of user documentation;
- System changeover; and
- Evaluation of the system a regular intervals.

**Equipment Installation:**
The hardware required to support new system is selected prior to this phase. Necessary hardware should be ordered & tested in time to allow installation. *An installation checklist should be developed with operating advice from vendor & developer*.
It involves:

- **Site Preparation:** An appropriate location & prescribed equipment (power backup, AC, etc.) must be availed to provide an operating environment.
- **Installation of New Hardware / Software:** The equipment must be physically installed by the manufacturer, connected-to the power source & wired to communication lines, if required.
- **Equipment Checkout:** The equipment must be turned on for testing under normal operating conditions. Though vendor conduct 'diagnostic tests', the implementation in-house team should conduct 'extensive tests' to ensure equipment functionalities in actual working conditions.

**Training Personnel:**
A system can succeed or fail depending on the way it is operated & used. Training is a major component of systems implementation. When a new system is acquired, which often involves new hardware & software, both users & computer professionals generally need some type of training.

**System Change-Over Strategies:**
Conversion/changeover is the process of changing over or shifting over from old system (may be manual system) to new system.
4 types of popular implementation strategies:

- **Direct Implementation / Abrupt Change-Over:** With this strategy, changeover is done in one operation, completely replacing the old system in one go.
- **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. If one phase is successful then next phase is started, this process continued till the new system fully replaces the old one.
- **Pilot Changeover:** With this strategy, the new system replaces the old one in one operation but only on a small scale (say 1 Branch). If successful then pilot is extended until it replaces the old system completely. Any errors can be rectified or further beneficial changes can be introduced throughout the system with least disruption.
- **Parallel Changeover:** This is most secure method with both systems running in parallel over an introductory period. Both operate together independently. If all goes well, the old system is stopped & new system carries on as the only system.

**Conversion Activities:**
Changeover or Conversion includes all those activities, which must be completed to successfully convert from previous system to new IS. These activities can be classified as:

- **Procedure Conversion:** Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, output & IC must be presented in clear, concise & understandable terms. Written operating procedures must be supplemented by oral communication during training sessions on system change.
- **File Conversion:** Because large files of information must be converted from one medium to another, this phase should be started long before programming & testing phase. Existing computer files should be kept for period of time until sufficient files are accumulated for backup in case of recovery after a "bug" is discovered later in conversion process.
- **System conversion:** After completing above conversion, daily processing can be shifted from existing IS to new one. A cut-off point is established so that database can be updated to the cut-off point. All transactions initiated after this time are processed on new system. System development team should be present to assist & to answer any questions that might develop. One should operate both system for some more time to match & check results of both system and all differences must be reconciled.
- **Scheduling Personnel & Equipment:** Scheduling data processing operations of a new IS for first time is difficult task. As users become more familiar with new system, the job becomes more routine. Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment.

# CHAPTER – 5 ACQUISITION, DEVELOPMENT & IMPLEMENTATION OF INFORMATION SYSTEM

## POST IMPLEMENTATION REVIEW & SYSTEMS MAINTENANCE

*As no phase may be assured to be perfect, errors are liable to occur. Thus, a well-formalized review must be undertaken including some of the systems maintenance activities*.
The deliverable of this phase, a well written document stating observations, modifications, scope of further improvements etc.

**Post Implementation Review:** *A Post Implementation Review answers the question "Did we achieve what we set out to do in business terms?"*
2 basic dimensions of IS should be evaluated. First - whether newly developed system is operating properly. Second - whether user is satisfied with IS. Typical evaluations include:

- **Development Evaluation:** To check whether system was developed on schedule & within budget, if not evaluate possible reasons. *It requires schedules & budgets to be established in advance and that record of actual performance & cost be maintained*.
- **Operational Evaluation:** To check (operational aspects) whether hardware, software & personnel are capable to perform their duties. *It tries to answer the questions related to functional aspects of system*.
- **Information Evaluation:** *It evaluates the value of information provided or generated by IS.*

**System Maintenance:** The need for modification arises from a failure to anticipate/capture all the requirements during system analysis/design and/or from changing organizational requirements.
Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** It is anticipated & can be planned for ensuring operational continuity & avoidance of anticipated risks. E.g. Scheduled Scanning in Antivirus.
- **Rescue Maintenance:** It refers to previously undetected malfunctions that were not anticipated but now arises & require immediate solution. E.g. Failure of system due to hard disk crashing.
- **Corrective Maintenance:** It deals with fixing bugs in code or defects found during executions. E.g. Correcting a failure to process the last record in a file.
- **Adaptive Maintenance:** It consists of adapting software to changes in the environment, such as hardware or operating system. E.g. change due to govt. policies, business rule, software and hardware operating platforms.
- **Perfective Maintenance:** It deals with accommodating to new or changed user requirements & concerns functional enhancements to the system to increase system's performance or to enhance its user interface. E.g. Updation in ERP.
- **Preventive Maintenance:** It is concerned with the activities aimed at increasing system's maintainability, such as updating documentation, adding comments, and improving modular structure of the system.

## OPERATION MANUALS

It is user's guide, also commonly known as Operations Manual. It is intended to give assistance to people using a particular system. It is usually written by technical writers, programmers or other technical staff etc. It is most commonly associated with electronic goods, computer hardware & software. It includes:

- Cover / title & content page and copyright page;
- Preface / Index, containing details of related documents & information on how to navigate user guide;
- A troubleshooting section detailing possible errors or problems along with how to fix them;
- A FAQ (Frequently Asked Questions);
- Where to find further help & contact details;
- A guide on how to use main functions of the system.

## AUDITORS' ROLE IN SDLC

- The audit of systems under development can have 3 main objectives.
  - To provide an opinion on efficiency, effectiveness & economy of project management.
  - To assess the extent to which the system being developed provides for adequate audit trails and controls to ensure integrity of data processed & stored;
  - To assess the effectiveness of controls being enacted for management of the system's operation.
- To achieve these goals, *an auditor has to attend steering committee meetings, examine project control or system documentation & conduct interviews*.
- *Auditor should provide a list of standard controls like response time, CPU usage & RAM availability etc. that the auditor has used as assessment criteria*.
- *Auditor may adapt a rating system e.g. 1 to 10 to give rating to various phases of SDLC, to form opinion about the SDLC phases.*
- *To audit technical work* (such as database design or physical design), *he may opt to take opinion from a technical experts*.
- Control considerations for an auditor include:
  - Documented policy & procedures;
  - Developers/ IT managers are trained on the procedures ;
  - Appropriate approvals are being taken at identified mile-stones;
  - Development is carried as per standards;
  - Separate test environment for development/ test/ production / test plans;
  - Business owners testing & approval before system going live;
  - Adequate audit trails are provided in system; and
  - Appropriateness of methodologies selected & source code is properly secured.
- Further, *Post-Implementation Review is performed to determine whether the system adequately meets earlier identified business requirements & needs*. Auditors should:
  - Determine if *expected benefits of new system are realized & users are satisfied with new system*.
  - Review which of the *SDLC phases have not met desired objectives & whether any corrective actions were taken*.
  - If there are *differences between expectations & actual results, determine reasons for the same* & offer guidelines for future projects.


(rajveer.an.indian@gmail.com)

# CHAPTER – 6 AUDITING OF INFORMATION SYSTEMS

## WHY CONTROLS & AUDIT

**Need for Audit of Information Systems**

FACTORS INFLUENCING AN ORGANIZATION TOWARD CONTROLS & AUDIT OF COMPUTERS.

- **Organisational Costs of Data Loss:** Data is critical resource for surviving in changing environment.
- **Incorrect Decision Making:** High level decisions require accurate data to make quality decision.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares & unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **Value of Computer Hardware, Software & Personnel*:*** These are critical resources, it has credible impact on its infrastructure & business competitiveness.
- **High Costs of Computer Error:** Data error during entry / process would cause great damage.
- **Maintenance of Privacy:** Data collected in business contains private information about an individual.
- **Controlled evolution of computer Use:** Use of technology & reliability of complex computer systems cannot be guaranteed, & consequences of using unreliable systems can be destructive.

**Major Objectives of IS Auditing / IS Audit Objective:**

- **Asset Safeguarding:** IS assets (hardware/software, data/information etc.) must be protected by internal controls from unauthorised access.
- **Data Integrity:** It is fundamental attribute of IS Auditing. It is important to maintain integrity of data of organisation.
- **System Effectiveness**: It refers to characteristics & objective of system to meet user requirements.
- **System Efficiency:** To optimize the use of various information system resources (E.g. Machine time).

**EFFECTS OF COMPUTER ON AUDIT**: To cope up with new technology usage in enterprise, auditor should be competent to provide independent evaluation as to whether business process activities are recorded & reported according to established standards or criteria.

**Changes to Evidence Collection:**

- **Data retention & storage:** Client's storage capacity may restrict the amount of historical data that can be retained "on-line" & readily accessible to auditor. Auditor may not be able to review whole reporting period transactions on computer system. E.g. Data may be stored in monthly / weekly summarized transactions or period closing balances.
- **Absence of input documents:** Transaction data may be entered into the computer directly without presence of supporting documentation. E.g. Online transactions.
- **Non-availability of audit trail:** Audit trails may not exist or may exist for short period of time. Absence of audit trail will make auditor's job very difficult & may call for an audit approach which involves *Auditing Around Computers* by seeking other sources of evidence to provide assurance that input has been correctly processed by computer system.
- **Lack of availability of printed output:** Transaction processed may not produce hard copy of output. Auditor have to access electronic data retained on client's computer by granting "read" access (given by client) to required files.
- **Audit evidence:** Some transactions may be generated automatically by computer system & may not have audit evidence. E.g. Depreciation.
- **Legal issues:** Using computer can create problems with contracts, e.g. when contract is made, where it is made (legal jurisdiction), what are terms of contract & parties to contract. Law regarding admission of electronic evidences varies from country to country / state to state / court to court.

**Changes to Evidence Evaluation:**

- **System generated transactions:** Systems may have ability to initiate, approve & record financial transactions.
- **Automated transaction processing** systems can cause problems for auditor. E.g. In 'just in time' (JIT) inventory & stock control systems: When stock level falls below certain level, system automatically generates purchase order & sends it to supplier with or without authorization of purchase manager.
- **Systemic Error:** Computers are designed to carry out processing on consistent basis. Given the same inputs & programming, they invariably produce same output.

If computer program is wrong, it will continuously give wrong output till is corrected.

**RESPONSIBILITY FOR CONTROLS:**

- Management is responsible for **establishing & maintaining control to achieve objectives of effective & efficient operations**.
- There are three levels **senior, middle & supervisory**.
  **Senior management** is responsible for strategic planning & objectives.
  **Middle management** develops tactical plans, activities & functions that accomplish strategic objectives.
  **Supervisory management** oversees & controls daily activities & functions of the tactical plan.

# CHAPTER – 6 AUDITING OF INFORMATION SYSTEMS

## IS AUDIT

IS Audit of an Information System environment may include one / both of following:

- **Assessment of internal controls within IS environment** to assure validity, reliability, & security of information & information systems.
- **Assessment of efficiency & effectiveness of IS environment**.

IS audit process is **to evaluate adequacy of internal controls** w.r.t. both specific computer program & data processing environment as a whole.

### SKILL OF IS AUDITOR

Audit objective & scope has significant bearing on skill & competence requirements of IS auditor. The set of skills that is generally expected;

- knowledge of **business operation, practices & compliance** requirement;
- Understand **technical & manual controls** relating to business continuity;
- Possess requisite professional **qualification, certification** & **experience** ;
- Understanding of **information Risks & Controls**;
- Knowledge of **IT strategies, policy & procedural controls**;
- Knowledge of **Professional Standards & Best Practices** of IT controls & security.

### FUNCTION OF IS AUDITOR

IS Auditor often is assessor of business risk. IS Auditor makes sound assessment & present risk-oriented advice to management.

IS AUDITORS REVIEW RISKS RELATING TO IT SYSTEM & PROCESSES:

- **Inadequate information security controls** (e.g. no antivirus, no / weak password)
- **Inefficient use of resources** (e.g. unnecessary expending on high power servers or workstations)
- **Ineffective IT strategies, policies & practices** (e.g. lack of Internet usage policy)
- **IT-related frauds** (e.g. phishing, hacking)

### CATEGORIES (Types) OF IS AUDIT (5 types)

- **Systems & Application:** To verify that systems & applications are appropriate, efficient, & adequately controlled.
- **Information Processing** (Online / Batch)**:** To verify that processing facility is controlled to ensure timely, accurate, & efficient processing under normal & potentially disruptive conditions.
- **Systems Development:** To verify that systems under development meet objectives of organization & developed in accordance with generally accepted standards for systems development.
- **IT Management & Enterprise Architecture:** To verify that IT management has developed organizational structure & procedures to ensure controlled & efficient environment for information processing.
- **Telecommunications, Intranets, & Extranets:** To verify that controls are in place on client, server, & on network connecting clients & servers.

### STEPS (Stages) IN IS AUDIT

- **Scoping:** Determining main areas of focus & any areas explicitly out-of-scope. Information sources include background reading & web browsing, previous audit reports, pre audit interview, observations.
- **Planning:** Scope is broken down into greater levels of detail, usually involves generation of audit work plan or risk-control-matrix.
- **Fieldwork:** Gathering evidences by interviewing staff & managers, reviewing documents, & observing processes etc.
- **Analysis:** Sorting out, reviewing & trying to make sense of all that evidences gathered earlier.
- **Reporting:** Reporting to management is done after analysis of evidences.
- **Closure:** Preparing notes for future audits & follow up with management.

### AUDIT STANDARDS & BEST PRACTICES

- **ISACA (Information Systems Audit & Control Association):** ISACA developed the following to assist IS auditor.
  - **IS auditing standards**
  - **IS auditing guidelines**
  - **IS auditing procedures**
  - **COBIT**
- **ISO 27001:** It is **international best practice** & **certification standard** for ISMS. ISMS is a systematic approach to manage Information security in an IS environment. ISO 27001 define how to organize Information Security in any kind of org. Companies certified generate greater client assurance. (INFOSYS, TCS, WIPRO are ISO certified)
- **Internal Audit Standards** issued by **IIA** (The Institute of Internal Auditors).
- **Standards on Internal Audit issued by ICAI** which specify process to be adopted by internal auditor in specific situation.
- **Information Technology Infrastructure Library (ITIL):** ITIL is set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business.

# CHAPTER – 6 AUDITING OF INFORMATION SYSTEMS

## PEFORMING IS AUDIT

### GENERAL POINTS

- IS Auditor uses **concepts of materiality & significance** to determine NTE of AP
- Materiality & significance **depends on quantity & quality**.
- **Planning occurs throughout audit** as an iterative process (based on findings).
- Objective of planning is to obtain **understanding of entity, its operations & internal control**.
- Devise **auditing testing plan & testing methodology** to determine whether **previously identified controls are effective**.
- Conduct several **tests with both valid & invalid data to test ability & extent of error detection, correction, prevention** within system.
- Key audit concern is that the **testing** should **reveal** any type of **exposure of sensitive data & information produced is valid, intact, & correct**.

### WAYS OF VALIDIATION OF INFORMATION

- **Asking same question to different personnel** & comparing answers;
- **Asking same question in different ways** at different times;
- **Comparing checklist** answers with **work papers** or other verifiable results;
- **Comparing checklist** answers with **observations** & **actual system results**;
- Conducting **mini-studies of critical phases** of operation.

### BASIC PLAN

- Planning is **important phases** of IS Audit. Its objective is to **optimize** use of audit resources.
- Adequate planning ensures that appropriate attention is devoted to **important areas** of audit, those **potential problems** are identified & work is **completed** expeditiously.
- Planning also assists in **proper assignment** of work to assistants & in **coordination** of work done by other auditors & experts.
- **Extent** of planning vary with **size / complexity** of entity & auditor's **experience** with entity & knowledge of business.
- Obtaining **knowledge of business** is important for planning to identify events, transactions & practices having material effect on FS.
- **Discuss** elements of overall audit plan & audit procedures with **AC/Management** to improve effectiveness & efficiency of audit.
- Audit Plan will need to be **sufficiently detailed to guide** development of audit program but in precise form & content
- **Modify audit plan** (i.e. Change in AP & its methodology initially planned) as changes in conditions / circumstances or unexpected findings during audit.
- **Document** audit plan & changes along with reason.

**PRELIMINARY REVIEW:** It helps auditor to gain clarity on objectives & scope of audit.

**1. Knowledge of the Business:**

- Economic factors & industry conditions,
- Nature of Business, its products & services,
- Exposure to business,
- Its clientele, vendors, strategic business partners/associates to whom critical processes have been outsourced,
- Level of competence of Top management & IT Management.

**2. Understanding the Technology:**

- Business processes & level of automation,
- Extent of dependence of enterprise on IT,
- Technology architecture such as distributed architecture, centralized architecture or hybrid architecture,
- Network diagrams to understand physical & logical network connectivity,
- SCM, CRM, ERM with which organization systems connect with its stakeholders,
- Various technologies and their advantages & limitations (e.g. authentication risks relating to e-mail system),
- IT policies, standards, guidelines & procedures.

**3. Understanding Internal Control Systems** by performing compliance & substantive testing.

**4. Legal Considerations & Audit Standards:**

- Evaluate legal & statutory implications on audit work.
- Statutory requirements, regulations & guidelines to conduct audit.
- Compliance with statutes or regulatory conditions as regards to minimum set of control objectives to be achieved by organization.
- Applicable Audit Standards. Non-compliance will be violation of Code of PE & will have adverse impact on auditor's work.

**5. Risk Assessment (RA) & Materiality:** RA is process of identifying risk, assessing risk, & recommending controls to reduce such risk to an acceptable level. RA allows auditor to determine scope of audit & assess level of audit risk.

THE KEY STEPS THAT CAN BE FOLLOWED FOR RISK-BASED APPROACH TO MAKE AN AUDIT PLAN:

- List IS used in organization & categorize them.
- Determine which systems impact critical functions or assets.
- Assess what risks affect these systems & severity of such impact on business.
- Based on above assessment, decide audit priority, resources, schedule & frequency.

**Risks are categorized as follows:**

- **Inherent Risk:** It is susceptibility of information resources or resources controlled by IS to material theft, destruction, disclosures, unauthorized modification, assuming that there are no related IC. (E.g. Inherent risk would be high in case of auditing of internet banking as compared to branch banking)
- **Control Risk:** Risk that material error, individually or in aggregate, will not be prevented or detected & corrected on timely basis by IC system.
- **Detection Risk:** Risk that IT auditor's substantive procedures will not detect error which could be material, individually or in aggregate. (E.g. Detection risk associated w.r.t. identifying breaches of security in an application system is high because logs for whole period may not available at the time of audit)

# CHAPTER – 6 AUDITING OF INFORMATION SYSTEMS



**INHERENT LIMITATION OF AUDIT**

**Documentation by Auditor**

To prepare proper report, auditor needs documented evidences which are not available in physical form.

To address this problems:

- Use of special audit techniques for documenting evidences. (E.g. CAAT)
- Audit timing to validate transactions as they occur.

**Inherent Limitation of Audit**

As per SA 200 any opinion formed by auditor is subject to inherent limitations of an audit:

- Nature of financial reporting;
- Nature of audit procedures;
- Need for the audit to be conducted within reasonable time & at reasonable cost.
- Fraud involving senior management or collusion.
- Related party relationships & transactions.
- Non-compliance with various laws & regulations.
- Future events or conditions affecting going concern.

**CONCURRENT & CONTINUOUS AUDIT**

Today, organizations produce information on real-time & online basis. Real-time recordings need real-time auditing to provide continuous assurance about the quality of data. Continuous auditing enables auditors to significantly reduce or eliminate the time b/w occurrence of events & its auditing. Errors in a computerized system are generated at high speeds and the cost to correct & rerun programs are high. If these errors can be detected & corrected at the point or closest to the point of their occurrence the impact would be least. Continuous auditing techniques use two bases for collecting audit evidence.

1. Use of embedded modules in system to collect, process & print audit evidence,
2. Special audit records used to store the audit evidence collected.

**Types of Audit Tools:**

**(i) Snapshots:** *Snapshot software is built into system at those points where material processing occurs which takes images of flow of any transaction as it moves through application.* These images are used to assess authenticity, accuracy, & completeness of the transaction processed. Main areas to focus:

1. To locate snapshot at material points & when snapshot will be captured
2. Reporting system design & its implementation to present data in meaningful way.

**(ii) Integrated Test Facility (ITF):** *ITF technique involves creation of dummy entity in the application system files to audit the processing of test data entered in dummy entity to verify processing authenticity, accuracy, & completeness*. Auditor has to decide method to be used to enter test data & methodology for removal of its effects.

**Methods of Entering Test Data:**

**1.** Transactions to be tested have to be tagged. Application system has to be programmed to recognize the tagged transactions & have them invoke two updates, one to application system master file record & one to ITF dummy entity.

**2.** Auditors may also use specifically prepared test data but it is time consuming & costly. It is likely to achieve more complete coverage than selected production data & application system does not have to be modified to tag ITF transactions & to treat them in a special way.

**Methods of Removing the Effects of ITF Transactions:**

**1.** Application system may be programmed to recognize ITF transactions & to ignore them in terms of any processing that might affect users.

**2.** Submit additional inputs that reverse the effects of ITF transactions.

**3.** Submit trivial entries so that effects of the ITF transactions on output are minimal. (Effects are not really removed)

**(iii) System Control Audit Review File (SCARF):** *SCARF technique 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- **SCARF master files**. Auditors then examine the information contained on such file to take follow-up. SCARF is like snapshot along with other data collection capabilities. Auditors might use SCARF to collect following types of information:

- **Application System Errors** - It check quality of system processing, whether there are any design & programming errors.
- **Policy & Procedural Variances** – It check when variations from policies, procedures & standards have occurred.
- **System Exception** - It monitors different types of application system exceptions.
- **Statistical Sample** -It provides a convenient way of collecting all sample information together on one file & use analytical review tools thereon.
- **Snapshots & Extended Records** - Snapshots & extended records can be written into the SCARF file & printed when required.
- **Profiling Data** – It can be used to collect data to build profiles of system users. Deviations from it will be indicated as some errors or irregularities.
- **Performance Measurement** – It can be used to collect useful data for measuring or improving the performance of an application system.

**(iv) Continuous & Intermittent Simulation (CIS):** *CIS can be used to trap exceptions whenever application system uses a DBMS*.

During application system processing, CIS executes in following way:

- DBMS reads an application system transaction. It is passed to CIS. CIS then determines whether it wants to examine the transaction further. If yes, next steps are performed or otherwise it waits to receive further data from DBMS.
- CIS replicates or simulates the application system processing.
- Every update to database arising from processing of selected transaction will be checked by CIS to determine whether any discrepancies exist b/w the results it produces & those the application system produces.
- Exceptions identified by CIS are written to an exception log file.
- Advantage of CIS is that it does not require modifications to application system & yet provides an online auditing capability.

**(v) Audit Hooks:** *These are audit routines that flag suspicious transactions*. E.g. Internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud, it led to change in name & address as soon as the policy was about to mature. Auditor devised a system of audit hooks to tag records with a name or address change, auditors will be informed of questionable transactions by as soon as they occur via real-time notification (displays a message on auditor's terminal).

**Advantages of Continuous Auditing:**

- **Cost & Time saving** – Reducing the cost of basic audit assignment by enabling auditors to test a larger sample (up to 100 %) of client's transactions & examine data faster & more efficiently than the manual testing;
- **Increase quality of audits** – Auditors can focus more on understanding client's business & its IC structure;
- **Specify transaction selection criteria** to choose transactions;
- Perform both **tests of controls & substantive tests** throughout the year on an ongoing basis.
- **Timely, Comprehensive & Detailed Auditing** – Evidence would be available more timely & in a comprehensive manner. Entire process can be evaluated & analyzed rather than examining inputs & outputs only.
- **Surprise test capability** – As evidences are collected from system itself by using CAT, auditors can gather evidence without systems staff & application system users being aware that evidence is being collected at that particular moment.
- **Information to system staff on meeting of objectives** - It provides information to systems staff regarding test vehicle to evaluate whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness & efficiency.
- **Training for new users** – New users can submit data & obtain feedback on any mistakes they make via system's error reports.

**Disadvantages of Continuous Auditing:**

- Auditors should be able to obtain resources required from organization to support development, implementation, operation, & maintenance of CAT.
- CAT is more effective if auditors are involved in development of application system.
- Auditors need knowledge & experience of working with computer systems to use CAT effectively & efficiently.
- CAT is used where audit trail is less visible and costs of errors & irregularities are high.
- CAT is ineffective if implemented in an unstable application system.

**AUDIT TRAIL**

***Audit trails*** *are logs that can be designed to record activity at the system, application, & user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives*. ***Audit trail controls*** *attempt to ensure that a chronological record of all events that have occurred in a system is maintained*.

The **Accounting audit trail** *shows the source & nature of data & processes that update the database*.

The **Operations audit trail** *maintains a record of attempted or actual resource consumption within a system.*

**Audit Trail Objectives:**

- **Detecting Unauthorized Access to System***: The primary objective of real-time detection is to protect system from outsiders who are attempting to breach system controls, indicate infestation by virus or worm. Real - time detection can impose a significant overhead on the operating system, which can degrade its performance.* Logs can be stored electronically & reviewed periodically. It can also be used to determine if unauthorized access was accomplished, or attempted and failed.
- **Facilitating Reconstruction of Events***:* Audit trail analysis helps to reconstruct the steps that led to events such as system failures, security violations or application processing errors and to avoid similar situations in the future.
  E.g. By maintaining record of all changes to account balances, audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Promoting Personal Accountability***:* Audit trails can be used to monitor user activity. Individuals will not violate security policy if they know that their actions are being monitored.

**Implementing an Audit Trail:**

Information contained in audit logs is useful for measuring the potential damage & financial loss associated with application errors, abuse of authority, or unauthorized access by outside intruders. Logs also provide valuable evidence or assess adequacies of controls in place & need for additional controls. Important information can easily get lost among the superfluous detail of daily operation. Thus, poorly designed logs can actually be dysfunctional.

**AUDIT & EVALUATION TECHNIQUES FOR PHYSICAL & ENVIRONMENTAL CONTROL**

**ROLE OF IS AUDITOR IN PHYSICAL ACCESS CONTROLS:** Auditing physical access requires the auditor to review physical access risk & controls:

- **Risk Assessment:** Auditor must satisfy that, RAP covers periodic assessment of all assets, physical access threats, vulnerabilities of safeguards & exposures there from.
- **Controls Assessment:** Based on risk profile, evaluate whether physical access controls are in place & adequate to protect the IS assets against the risks.
- **Review of Documents:** Examine relevant documents such as security policy & procedures, premises plans, building plans, inventory list & cabling diagrams.

**AUDIT OF ENVIRONMENTAL CONTROLS**

**Role of Auditor in Environmental Controls:** The attack on World Trade Centre in 2001 has created a worldwide alert bringing focus on BCP & environmental controls. Audit of environmental controls should form a critical part of every IS audit plan. Some of critical audit considerations that an IS auditor should take into account while conducting audit:

**Audit Planning & Assessment:** As part of risk assessment:

- Risk profile should include different kinds of environmental risks (both natural & man-made threats) that the organization is exposed to.
- Periodically reviewed the risk profile to ensure updation with newer risks.
- Ascertain - controls safeguard against all acceptable risks are in place.
- Review security policy to assess policies & procedures that safeguard the organization against environmental risks.
- Review building plans & wiring plans to determine appropriateness of location, review of surroundings, power & cable wiring etc.
- Interview relevant personnel about awareness of environmental threats & controls, their role of in environmental control procedures.

**Audit of Environmental Controls:** Physical inspections & observe practices.

- Type of materials used for construction;
- Presence of water & smoke detectors, power supply arrangements;
- Location of fire extinguishers, firefighting equipment & refilling date;
- Emergency procedures, evacuation plans & marking of fire exists;
- Documents for compliance with legal & regulatory requirements;
- Review effectiveness of power conditioning equipment & generators.
- Check power supply interruptions to test effectiveness of back-up power;
- Environmental control equipment such as AC, dehumidifiers, heaters, etc.;
- Assess whether time gap b/w Failures & Repair are within acceptable levels;
- Identify undesired activities such as smoking, consumption of eatables etc.

**Documentation:**

Document all findings. Working papers could include:

- Audit assessments,
- Audit plans,
- Audit procedures,
- Questionnaires,
- Interview sheets,
- Inspection charts etc.

# CHAPTER – 6 AUDITING OF INFORMATION SYSTEMS

| MANAGERIAL CONTROLS & THEIR AUDIT TRAILS | |
|---|---|
| **Top Management & Information Systems Management Controls** | Top management's role in POLC IS Function. Advise them w.r.t. to long-run policy decision making & translates long-run policies into short-run goals & objectives.<br>• **Planning:** Auditors need to evaluate whether top management has formulated a high-quality IS's plan that is appropriate to the needs of an organization or not.<br>• **Organizing:** Auditors should be concerned about how well top management acquires & manages staff resources.<br>• **Leading:** Auditors examine variables that often indicate when motivation problems exist or suggest poor leadership. E.g. frequent failure of projects to meet their budget. Auditors may use both formal sources (IS plans, Documents standard, Policies) and informal sources (Interview) of evidence to evaluate how well top mangers' communicate with their staff.<br>• **Controlling:** Auditors must evaluate whether top management's choice to means of control over users of IS services is likely to be effective or not. |
| **System Development Management Controls** | 3 types of audits may be conducted during system development process<br>**Concurrent Audit -** Auditors are members of System Development Team. Auditor assist the team in improving the quality of systems development for specific system they are building & implementing. [Management might require Internal Auditor to participate in development of material application systems]<br>**Post - implementation Audit -** Auditors seek to help an organization learn from its experiences in the development of a specific application system. Evaluate whether the system needs to be scrapped, continued, or modified. [Management might require Internal Auditor to undertake post-implementation reviews of material application systems]<br>**General Audit -** Auditors seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to FS for systems effectiveness & efficiency. [An external auditor is more likely to undertake general audits] |
| **Programming Management Controls** | Phases in program life cycle & important controls to be exercised in each phase.<br>**Planning –** Evaluate whether nature & extent of planning are appropriate and how well the planning work is being undertaken.<br>**Control –** Evaluate whether nature & extent of control activities undertaken are appropriate for different types of software being developed or acquired. Gather evidence on whether the control procedures are operating reliably<br>**Design –** Find out whether programmers use some type of systematic approach to design by undertaking interviews, observations, and reviews of documentation.<br>**Coding –** Auditors should seek evidence –<br>○ On the level of care exercised in choosing a module implementation & integration strategy.<br>○ To determine whether programmers follow structured programming conventions.<br>○ To check whether programmers employ automated facilities to assist them with their coding work.<br>**Testing –** Auditor's primary concern is to see that unit testing; integration testing of system testing has been undertaken appropriately.<br>**Operation & Maintenance –** Ensure effectively & timely reporting of maintenance needs occurs & maintenance is carried out in a well-controlled manner and management has implemented a review system. |
| **Data Resource Management Controls** | Role of database administrator.<br>• Determine what controls are exercised to maintain data integrity. Interview database users to determine their level of awareness of these controls.<br>• Employ test data to evaluate whether access controls & update controls are working. |
| **Quality Assurance Management Controls** | Functions performed by QA Management to ensure development, implementation, operation & maintenance of IS conform to quality standards.<br>Auditor might use interviews, observations & reviews of documentation to evaluate how well QA Personnel perform their *monitoring* role, make *recommendations* for improved standards or processes, and their *reporting* function. |
| **Security Management Controls** | Functions performed by Security Administrators to identify threats to IS functions & to design, implement, operate & maintain controls that reduce expected losses to an acceptable level.<br>Evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; and check whether organizations have opted appropriate Disaster recovery & Insurance plan or not. |
| **Operations Management Controls** | Functions performed by Operations Management to ensure day-to-day operations of IS function are well controlled.<br>Auditor should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel. |

| APPLICATION CONTROLS & THEIR AUDIT TRAILS | | | | | |
|---|---|---|---|---|---|
| **Boundary Controls:** | **Input Controls:** | **Communication Controls:** | **Processing Controls:** | **Database Controls:** | **Output Controls:** |
| Establishes interface b/w user & system itself. System must ensure that it has an authentic user.<br>Users are allowed to use resources in restricted ways. | Responsible for bringing data & instructions into IS.<br>Input Controls are validation & error detection of data input into system. | Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls. | Responsible for computing, sorting, classifying & summarizing data.<br>It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results. | Responsible to provide functions to define, create, modify, delete & read data in an IS.<br>It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions. | To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared & routed to users. |

# CHAPTER – 6 AUDITING OF INFORMATION SYSTEMS

**Audit Trail Controls:** Two types of audit trails that should exist in each subsystem are as follows:

- **Accounting Audit Trail** to maintain a **record of events** within subsystem; &
- **Operations Audit Trail** to maintain a record of **resources consumption associated with each event** in subsystem.

*(Note: Audit Trails for Application Control have been discussed above)*

## AUDIT OF APPLICATION SECURITY CONTROL

The objective of this exercise is to establish whether application security controls are operating effectively to protect CIA of information. The lacunae in application security may lead to security related frauds that may result in financial & reputation losses.

### APPROACH TO APPLICATION SECURITY AUDIT

Application security audit is being looked from usage perspective. A layered approach is used, which is based on the activities undertaken at various levels of management (Supervisory, Tactical & Strategic)

For this, Auditors need to have a clear understanding of the following.

- Business process for which the application has been designed;
- Source of data input to & output from the application;
- Various interfaces of the application under audit with other applications;
- Various methods used to login to application, other than normal user-id & passwords used;
- The roles, descriptions, user profiles & user groups that can be created in an application;
- Policy for user access & supporting standards.

**Various Layer**

- **Operational Layer:** Basic layer, where user access decision are generally put in place.
- **Tactical Layer:** Next is management layer, which includes supporting functions e.g. security administration, IT risk management, etc.
- **Strategic Layer:** Layer used by TOP management. It includes the overall information security governance, security awareness, supporting information security policies & standards.

### UNDERSTANDING THE LAYERS OF SECURITY & RELATED AUDIT ISSUES

(i) **Operational Layer:** The operational layer audit issues include:

- **User Accounts & Access Rights:** It includes defining unique user accounts & providing them access rights as per their roles & responsibilities. Auditor should ensure the use of unique user IDs & these should be traceable to individual for whom created.
- **Password Controls:** It includes strength, minimum length, age, non-repetition of password & automated lockout after 3 attempts. Auditor should check whether password controls are weak, if yes, then look for compensating controls against such issues.
- **Segregation of Duties:** As frauds due to collusions / lack of segregations increase across the world, importance of Segregation of Duties also increases. It prevents or detects errors & irregularities by assigning separate individuals' responsibility for initiating & recording transactions & custody of assets to separate individuals. E.g.
  - Record keeper of asset must not be asset keeper.
  - Cashier who creates a cash voucher in system, must not have right to authorize payments.
  - Maker must not be checker.

  Auditor needs to check that there is no violation of above principle. Any violation should be immediately communicated to TCWG.

(ii) **Tactical Layer:** At the tactical layer, security administration is put in place. This includes:

- **Timely updates to user profiles**, like creating/deleting & changing of user accounts. Auditor should ensure that any change to user rights is done through a formal process E.g. approval senior management.
- **IT Risk Management:** it includes:
  - Assessing risk over key application controls;
  - Conducting regular security awareness programme;
  - Enabling application users to perform a self-assessment/complete compliance checklist questionnaire to estimate the users' understanding about application security;
  - Reviewing application patches before deployment & regularly monitoring critical application logs;
  - Monitoring peripheral security e.g. updating antivirus software;

  Auditor should understand the risk associated with each application & obtain periodic risk assessment report or self-assessment/ compliance reports on the application.
- **Interface Security:** It relates to application interfaced with another application in organization. Auditor should understand the data flow to & from application. Security of interfaced data is important when unencrypted methods of data transmission are used.
- **Audit Logging & Monitoring:** Audit logs should be regularly monitored. Same is not possible for all transactions, so it must be done on an exception reporting basis.

(iii) **Strategic Layer:** At this layer, Top Management forms security policy & guideline supported & supplemented by detailed standards & guidelines. A comprehensive information security programme fully supported by top management & communicated well to the organization is importance to succeed in information security.

One of key responsibilities of IT risk management function is to promote ongoing security awareness to organization's users. Auditor needs to check whether all these aforementioned guidelines have been properly framed & capable of achieving business objectives.

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUSES

**Role of Auditor in IT Act**

To an auditor, it is important to understand key provisions of IT Act as it impacts other compliances & provides basis for other compliances. E.g. As per companies Act, specific aspects of internal controls & risk management are to be reviewed by auditor.

In modern enterprises, most critical information is input, processed & stored in computers or in electronic forms. Hence, risks of it being misused & non-compliance of regulatory provisions has to be understood & should also communicated to client to mitigate control weaknesses & ensure compliance.

**The Objectives of IT Act:**

- To grant legal recognition for transactions carried out by means of "e-commerce";
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
- To facilitate e-filing of documents with Government departments;
- To facilitate electronic storage of data;
- To facilitate & give legal sanction to electronic fund transfers b/w banks & financial institutions;
- To give legal recognition for keeping of books of accounts by banker's in electronic form; &
- To amend Indian Penal Code, Indian Evidence Act, Banker's Book Evidence Act & RBI Act.

**Key Definitions**

"**Asymmetric Crypto System**" means a **system of a secure key pair** consisting of a **private key for creating a digital signature** & a **public key to verify the digital signature**;

"**Digital Signature**" means **authentication of any electronic record by a subscriber** by means of an electronic method or procedure as per section 3;

"**Electronic signature**" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule & includes digital signature.

"**Electronic Form**" with reference to information, it means **any information generated, sent, received or stored in** media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

"**Intermediary**" w.r.t. any particular electronic records, it means any **person who on behalf of another person receives, stores or transmits that record or provides any service w.r.t. that record & includes** telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places & cyber cafes;

"**Key Pair**", in an asymmetric crypto system, **means a private key & its mathematically related public key**, which are so related that the public key can verify a digital signature created by the private key;

**[CHAPTER-II] DIGITAL SIGNATURE & ELECTRONIC SIGNATURE**

This chapter of IT Act gives legal recognition to electronic records & digital signatures. It provides conditions subject to which an electronic record may be authenticated by means of affixing digital signature.

The digital signature is created in two distinct steps.

I. Electronic record is converted into a message digest by using "**hash function**" which digitally freezes such electronic record to ensure integrity of content of such electronic record. Any tampering with such contents of electronic record will immediately invalidate digital signature.

II. Identity of person affixing digital signature is authenticated through use of a private key which attaches itself to message digest & which can be verified by anybody who has public key corresponding to such private key.

**[SECTION 3] AUTHENTICATION OF ELECTRONIC RECORDS**

I. Any subscriber may authenticate an electronic record by affixing his Digital Signature subject to this section.

II. Authentication of the electronic record shall be effected by use of **asymmetric crypto system & hash function** which envelop & transform the initial electronic record into another electronic record.
**"Hash function"** means an algorithm mapping or translation of one sequence of bits into another so that an electronic record yields same hash result every time the algorithm is executed.

III. By using public key of the subscriber, any person can verify the electronic record.

IV. Private Key & Public Key are unique to the subscriber & constitute a **functioning key pair**.

**[Section 3A] Electronic Signature**

I. Subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which- is **considered reliable; & specified in Second Schedule.**

II. Electronic signature / electronic authentication technique shall be considered reliable if-
   (a) Signature creation data or authentication data are linked to the signatory or authenticator & no other person;
   (b) At time of signing, signature creation data or authentication data were under control of the signatory or authenticator & no other person;
   (c) Alteration to **electronic signature** made after affixing such signature is detectable;
   (d) Alteration to **information** made after its authentication is detectable; and
   (e) Fulfills other conditions as may be prescribed.

III. CG may alter second schedule by notification in official gazette.



(rajveer.an.indian@gmail.com)

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUSES

**[CHAPTER III] ELECTRONIC GOVERNANCE:** It specifies procedures to be followed for sending & receiving of electronic records and time & place of dispatch & receipt.

| | |
|---|---|
| **[SECTION 4] LEGAL RECOGNITION OF ELECTRONIC RECORDS**<br>Where any law requires information to be in writing or printed form then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information is -<br>(a) in electronic form; &<br>(b) accessible for subsequent reference. | **[SECTION 5] LEGAL RECOGNITION OF ELECTRONIC SIGNATURES**<br>Where any law requires that any information or document to be authenticated by affixing the signature then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or document is authenticated by affixing electronic signature affixed in manner prescribed by CG. |
| **[Section 6] Use of Electronic Records & Electronic Signatures in Government & its agencies**<br>(1) Where any law provides for -<br>(a) filing of any form, application or document with government offices & it's agencies in particular manner;<br>(c) issue or grant license, permit, sanction or approval in particular manner;<br>(b) receipt or payment of money in particular manner,<br>Then notwithstanding anything contained in any other law, such requirement shall be deemed to have been satisfied if effected in e-form.<br>(2) Appropriate Government may prescribe manner & format & fee & charges for such e-form. | **[SECTION 7] RETENTION OF ELECTRONIC RECORDS**<br>(1) Where any law provides that documents, records or information shall be retained for any specific period, then requirement shall be deemed to have been satisfied if such documents, records or information are retained in electronic form, if -<br>(d) information contained therein accessible for subsequent reference;<br>(e) forms & format should not be changed;<br>(f) details which will facilitate identification of origin, destination, date & time of dispatch or receipt of such electronic record are available in the electronic record:<br>(2) This section do not apply where law expressly provides for retention of documents, records or information in e-form or where information automatically generated in e-form. |
| **[Section 6A] Delivery of services by Service Provider**<br>Service provider authorised by appropriate Government can provide services in e-form as per policy governing such service sector & can collect service charge as per scale of service charges given by appropriate Government. | **[Section 7A] Audit of Documents, etc. maintained in Electronic form**<br>Provision for audit of documents maintained in physical form are also applicable to documents, records or information maintained in e-form. |
| **[Section 8] Publication of rules, regulation, etc., in Electronic Gazette**<br>Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in Official Gazette or Electronic Gazette.<br>Date of publication shall be deemed to be date of Gazette which was first published in any form. | **[Section 10] Power of CG to make rules in respect of Electronic Signature**<br>The CG may prescribe by rules:<br>(a) Type of Electronic Signature;<br>(b) Manner & format in which Electronic Signature shall be affixed;<br>(c) Manner & procedure for identification of the person affixing Electronic Signature;<br>(d) Control processes & procedures to ensure adequate integrity, security & confidentiality of electronic records or payments; and<br>(e) Any other necessary matter. |
| **[Section 9] Sec 6, 7 & 8 not to confer right to insist document should be accepted in e-form**<br>No person can insist government department to accept, issue, create, retain & preserve any document in e-form. | **[Section 10A] Validity of contracts formed through electronic means**<br>Where in a contract, proposals, acceptance, revocation of proposals & acceptances are expressed in electronic form or means then such contract shall not be deemed to be unenforceable solely on ground that electronic form or means was used for that purpose. |

**[CHAPTER V] SECURE ELECTRONIC RECORDS & SECURE ELECTRONIC SIGNATURES:** It sets out conditions to qualify electronic records & digital signatures as being secure.

| | | |
|---|---|---|
| **[Section 14] Secure Electronic Record**<br>Where any security procedure has been applied to an electronic record at specific point of time, then such record shall be deemed to be secure electronic record from such point of time to the time of verification. | **[Section 15] Secure Electronic Signature**<br>An electronic signature deemed to be secure electronic signature if -<br>(1) At the time of affixing signature, signature creation data (i.e. Private Key) was under exclusive control of signatory & no other person; and<br>(2) Signature creation data was stored & affixed in prescribed manner. | **[Section 16] Security Procedures & Practices**<br>CG may prescribe security procedures & practices for the purposes of sections 14 & 15 considering commercial circumstances, nature of transactions & other related factors. |



(rajveer.an.indian@gmail.com)

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUES

**[CHAPTER IX] PENALTIES, COMPENSATION & ADJUDICATION**

**[Section 43] Penalty & Compensation for damage to computer, computer system, etc.**

If any person without permission of owner or person-in-charge of computer, computer system or computer network:

(a) **accesses** or secures access;
(b) **downloads**, copies or extracts any data, computer data base or information including information or data held or stored in removable storage media;
(c) introduces or causes to be introduced any computer **contaminant or virus**;
(d) **damages, disrupts** or causes to be damage, disruption;
(e) **denies** or causes denial of access to any person authorised to access;
(f) provides any **assistance to any person to facilitate access** in contravention;
(g) **charges services availed** of by a person to **account of another person** by tampering with or manipulating;
(h) **destroys, deletes, alters or diminishes** its value of any information residing in computer resource;
(i) **steals, conceals, destroys or alters** or (causes any person to) any computer source code used for a computer resource with an intention to cause damage.

he shall be liable to **pay damages** by way of compensation **to person so affected**.

**[Section 43A] Compensation for failure to protect data**

Where a **body corporate**, possessing, dealing or handling any sensitive personal data or information, is negligent in implementing & maintaining reasonable security practices & procedures & thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to **pay compensation for damages to affected person**.

**[Section 44] Penalty for failure to furnish information return, etc.**

If any person who is required & fails to -

(a) furnish any document, return or report to Controller or Certifying Authority- **Penalty upto Rs. 1,50,000/-**
(b) file any return or furnish any information, books or other documents within time specified- **Penalty upto Rs. 5,000/- per day.**
(c) maintain books of account or records- **Penalty upto Rs. 10,000/- per day.**

**[Section 45] Residuary Penalty**

Contravenes any rules or regulations for which no penalty separately provided-

- Compensation to affected person or
- Penalty

**Upto Rs. 25,000/-**

| [CHAPTER XI] OFFENCES | Imprisonment upto | Fine upto |
|---|---|---|
| **[Section 65] Tampering with Computer Source Documents**<br>Whoever **knowingly / intentionally** (causes another to) conceals, destroys or alters any computer source code. | **3 years** | **Or 2 lakh** |
| **[Section 66] Computer Related Offences**<br>If any person, dishonestly / fraudulently, does any act referred to in **section 43.** | **3 years** | **Or 5 lakh** |
| **[Section 66B] Punishment for dishonestly receiving / retaining stolen computer resource or communication device** knowing or having reason to believe that same is stolen. | **3 years** | **Or 1 lakh** |
| **[Section 66C] Punishment for identity theft**<br>Whoever, fraudulently or dishonestly make **use of electronic signature, password or other unique identification feature of other person**. | **3 years** | **Or 1 lakh** |
| **[Section 66D] Punishment for cheating by personation by using computer resource or communication device.** | **3 years** | **Or 1 lakh** |
| **[Section 66E] Punishment for violation of privacy**<br>Whoever, intentionally / knowingly captures, publishes or transmits **image of private area of any person without his/her consent**. | **3 years** | **Or 2 lakh** |
| **[Section 66F] Punishment for cyber terrorism**<br>Whoever commits offence of cyber terrorism –<br>A. with intent to **threaten unity, integrity, security or sovereignty of India or to strike terror in people or any section of people** by<br>i. denying or cause **denial of access** to any person authorised to access computer resource; or<br>ii. attempting to **penetrate or access computer resource** without authorisation or exceeding authorised access; or<br>iii. introducing or causing to introduce any **computer contaminant**,<br>**causing death or injuries** to persons or **damage or destruction** to property or disrupts or knowingly **damage or disruption** of supplies or services essential to life of the community; or<br>B. Knowingly or intentionally **penetrates or accesses computer resource** without authorisation or exceeding authorised access, & obtains access to restricted information, data or computer database **w.r.t. national or international matter**. | **Life time** | **-** |


(rajveer.an.indian@gmail.com)

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUSES

| | | |
|---|---|---|
| **[Section 67] Punishment for publishing or transmitting obscene material in electronic form**<br>Whoever publishes / transmits (or causes to be) in electronic form, any material which is lascivious (lustful) / appeals to prurient interest / if its effect is such as to tend to deprave & corrupt persons who are likely to read, see or hear the matter contained or embodied in it. | **First time- 3Y**<br>**Next time- 5Y** | **And 5 lakh**<br>**And 10 lakh** |
| **[Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form**<br>Whoever publishes / transmits (or causes to be) in electronic form any material which contains sexually explicit act / conduct. | **First time- 5Y**<br>**Next time- 7Y** | **And 10 lakh**<br>**And 10 lakh** |
| **[Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form**<br>Whoever, -<br>(a) publishes / transmits (or causes to be) material in any electronic form which depicts children engaged in sexually explicit act / conduct; or<br>(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or<br>(c) cultivates (adapt), entices (provoke) or induces (cause to do) children to online relationship with one or more children for & on sexually explicit act or in manner that offends a reasonable adult on computer resource; or<br>(d) facilitates abusing children online; or<br>(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children<br>**Section 67 / 67A /67B not extend** to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form -<br>(i) publication of which is justified for public good in interest of science, literature, art / learning; or<br>(ii) kept / used for bona fide heritage or religious purposes. | **First time- 5Y**<br>**Next time- 7Y** | **And 10 lakh**<br>**And 10 lakh** |
| **[Section 67C] Preservation & Retention of information by intermediaries**<br>(1) Intermediary shall preserve & retain prescribed information for specified duration in manner & format prescribed by CG.<br>(2) Any intermediary who intentionally / knowingly contravenes shall be punishable with | **3 years** | **And liable to fine** |
| **[Section 68] Power of Controller to give directions**<br>(1) To ensure compliance of this act, Controller may direct Certifying Authority or its employee to take such measures or cease carrying activities as specified in order<br>(2) Any person who intentionally / knowingly fails to comply with such order shall be guilty of offence. | **2 years** | **Or 1 lakh** |
| **[Section 69] Powers to issue directions for interception / monitoring / decryption of any information through any computer resource**<br>(1) In interest of sovereignty, integrity of India, defense of India, security of the State, friendly relations with foreign States or for investigation, CG/SG/Authorised officers may (reasons to be recorded in writing) direct any appropriate government agency to intercept / monitor / decrypt any information generated, transmitted, received or stored in any computer resource.<br>(2) Such subscriber / intermediary / any person-in-charge of computer resource shall extend all facilities & technical assistance, if fails... | **7 years** | **And also liable to fine** |
| **[Section 69A] Power to issue directions for blocking for public access of any information through any computer resource**<br>(1) In interest of sovereignty, integrity of India, defense of India, security of the State, friendly relations with foreign states, CG/Authorised officers may (reasons to be recorded in writing) direct any Government agency / intermediary to block access by public to any information generated, transmitted, received, stored or hosted in any computer resource.<br>(2) The intermediary who fails to comply shall be punishable with… | **7 years** | **And also liable to fine** |
| **[Section 69B] Power to authorise to monitor & collect traffic data / information through any computer resource for Cyber Security**<br>(1) To enhance Cyber Security / for identification / analysis & prevention of any intrusion or spread of computer contaminant in country, CG may authorise any government agency to monitor & collect traffic data or information generated / transmitted / received / stored in any computer resource.<br>(2) Intermediary or person in-charge of Computer resource shall provide technical assistance & extend all facilities to such agency, if intentionally / knowingly contravenes then … | **3 years** | **And also liable to fine** |
| **[Section 70] Protected system**<br>CG can declare any **Critical Information Infrastructure as Protected System**. Damage to Critical Information Infrastructure will cause huge impact on national security, economy, public health or safety. Any person who secures access / attempts to secure access to protected system in contravention of provisions of this section shall be … | **10 years** | **And also liable to fine** |
| **[Section 70A] National nodal agency**<br>CG may designate any Govt. org. as National nodal agency, which shall be **responsible** for all measures including Research & Development relating to **protection of Critical Information Infrastructure**. | | |



(rajveer.an.indian@gmail.com)

| | | |
|---|---|---|
| **[Section 70B] Indian Computer Emergency Response Team to serve as national agency for incident response**<br>• This team is established by CG for – collection, analysis & dissemination of information, forecast & alerts, emergency measures for handling, coordination, issue guidelines other matters on cyber incidents.<br>• Team may call for information & give direction to service providers, intermediaries, data centers, body corporate & any other person. If fails… | **1 years** | **Or 1 lakh** |
| **[Section 71] Penalty for misrepresentation / suppression of material fact for obtaining any license / Electronic Signature Certificate.** | **2 years** | **Or 1 lakh** |
| **[Section 72] Penalty for breach of confidentiality & privacy (Misuse of power by Govt. officials)**<br>Except with otherwise provided in this Act or any other law, any person in pursuance of any powers conferred under this Act has secured access to any electronic record, book, register, correspondence, information, document or other material without consent of owner. | **2 years** | **Or 1 lakh** |
| **[Section 72A] Punishment for Disclosure of information in breach of lawful contract**<br>Except with otherwise provided in this Act or any other law, any person / intermediary who, while providing services under terms of lawful contract, has secured access to any material containing personal information about another person & discloses without consent of person concerned to cause wrongful loss / gain, or in breach of contract. | **3 years** | **Or 5 lakh** |
| **[Section 73] Penalty for publishing Electronic Signature Certificate falsely**<br>No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person which is –<br>(a) Not issued by Certifying Authority or<br>(b) Not accepted by subscriber or<br>(c) Revoked or suspended by Certifying Authority. | **2 years** | **Or 1 lakh** |
| **[Section 74] Knowingly create, publish or otherwise make available an Electronic Signature Certificate for fraudulent / unlawful purpose.** | **2 years** | **Or 1 lakh** |
| **[Section 75] Provision of this act apply to any offences / contraventions committed outside India by any person irrespective of his nationality, if such act involves computer / computer system / computer network located in India.** | | |
| **[Section 76] Confiscation**<br>Any computer, computer system, floppies, compact disks, tape drives or any other accessories used in respect of contravention of any provision of this Act shall be liable to confiscation.<br>However, if it is proved that such resources were not used in committing such contravention then only person contravening would be arrested & none of computer resources would be confiscated. | | |

**[CHAPTER XII] INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES**

**[Section 79] Exemption from liability of intermediary in certain cases**

Intermediary shall not be liable for third party information / data / communication link made available or hosted by him if-

(a) function of intermediary is limited to providing access to communication system over which information made available by third parties is transmitted / temporarily stored / hosted; or

(b) intermediary does not –
  i. initiate transmission,
  ii. select receiver of transmission, and
  iii. select / modify information contained in transmission

(c) intermediary observes due diligence while discharging his duties.

**Not apply** if (i.e. liable) - Intermediary has conspired / abetted / aided / induced whether by threats / promise / otherwise in commission of unlawful act;

**[CHAPTER XIIA] EXAMINER OF ELECTRONIC EVIDENCE**

**[Section 79A] Central Government to notify (Any Dept. / Body / Agency of CG/SG) as Examiner of Electronic Evidence** for providing expert opinion on electronic evidence before any court / other authority.

**[CHAPTER XIII] MISCELLANEOUS**

**[Section 80] Power of police officer (NOT BELOW RANK OF INSPECTOR) & other officers (of CG/SG) to enter PUBLIC PLACE, search, & arrest any person without warrant** who is reasonably suspected of having committed / committing / about to commit any offence under this Act.
(Arrested by officer other than police officer - without unnecessary delay, take / send the person arrested before magistrate having jurisdiction / police station.)


(rajveer.an.indian@gmail.com)

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUSES

**[Section 81] This act to have Overriding effect to all laws except Copyright Act, 1957 & Patent Act, 1970**

**[Section 81A] Application of Act to electronic cheque & truncated cheque**

**[Section 84C] Punishment for ATTEMPT TO COMMIT OFFENCES (Where no express provision for punishment)**
**Imprisonment –** 1/2 of longest term of imprisonment, OR / AND
**Fine –** 100% Fine

**[Section 85] Offences by Companies**
Company & person (who was in charge of / was responsible to – for conduct of business of company) shall be guilty & liable for punishment.
However, such person shall not be liable if he proves that contravention took place without his knowledge / exercised all due diligence to prevent such contravention.

## REQUIREMENTS OF VARIOUS AUTHORITIES FOR SYSTEM CONTROLS & AUDIT

**Requirements of IRDA for System Controls & Audit: IRDA** is apex body overseeing insurance business in India. It protects interests of policyholders, regulates, promotes & ensures orderly growth of insurance business in India. IS Audit aims at providing assurance w.r.t. CIA for IS.

**System Audit:**
- At least **once in 3 years** by CA firm.
- For system audit - **Internal, concurrent or statutory auditor not eligible**.
- CA firm minimum of **3-4 years' experience** of IT systems of banks / MF / insurance co.

**Preliminaries:** (Obtain Info. About)
- **Location(s)** from where Investment activity is conducted.
- **IT Applications used** to manage Insurer's Investment Portfolio.
- **System layout** of IT & network infrastructure (Like Details of server, database, types of network connectivity, firewalls other facilities / utilities).
- Whether systems & applications are **hosted centrally or at different office**.
- **Previous Audit reports** & **unresolved issues**.
- **Internal circulars & guidelines** of Insurer.
- List of **new Products/funds introduced** along with IRDA approvals for same.
- **Lists of all investments** held on date.
- **Circulars & notifications** issued **by IRDA**.

**System Controls:** (There should be)
- Electronic **t/f of Data without manual intervention**.
- All Systems should be **seamlessly integrated**.
- **Audit Trail** at **every Data entry point**.
- Auditor should **comment on audit trail**.
- Procedures for **reviewing & maintaining audit trail**.
- **Separate logins** for each user & maintains **trail for every transaction** w.r.t. **authorization & modifications**.

**Requirements of RBI for System Controls & Audit: RBI** is India's central bank, which formulates monetary policy with regard to Indian rupee &:
- Regulate issue of banknotes,
- Maintain reserves to securing monetary stability, &
- Operate credit & currency system of country to its advantage.

RBI suggests that senior management & regulators need assurance on effectiveness of internal controls implemented.

**System Control:**
- **Duties of system programmer/designer** (only make modifications/improvements) **not to be assigned to operator** (only use) of system.
- **Contingency plans/procedures** in case of **failure of system** to be introduced/ tested by auditor at periodic intervals to evaluate its effectiveness.
- Appropriate **control measure devised & documented to protect system from attacks**.
- To bring **uniformity of software** used by various branches/offices, there should be a **formal method** (approved by senior management) **of incorporating changes in standard software**.
- BOD & senior management are responsible for ensuring **operating effectiveness of internal control** implemented.
- Annual **review of IS Audit Policy & its effectiveness**.
- Bank must conduct **Quality Assurance at least once 3 years**.

**System Audit:**
- Banks require **separate IS Audit function** within Internal Audit department led by IS Audit Head reporting to Head of Internal Audit.
- IS auditors must be **independent, professionally competent** (like CISA) **enough skill, knowledge & experience & exercise due professional care**.
- **Engagement letter should address independence & accountability of audit function**.
- **To ensure independence**, make sure:
  - Auditors have **access to information & applications**, and
  - Auditors have **right to conduct independent data inspection & analysis**.
- **IT Governance, information security governance, critical IT general controls**, etc. needs to be **subjected to IS Audit** at least **once in a year**.
- IS Audits should **cover large & medium branches** in areas like controls of passwords, user ids, segregation of duties, physical / logical security, review of exception reports or audit trails, etc.
- Review following additional areas:
  - **Testing controls** on new development systems **in live environment before implementing** them.
  - Consider **pre & post implementation review** of application controls.
  - Ensure **data integrity after implementation of new application / system** or in case of **data migration from legacy systems to new system** & validate IT risks in system before launch.
  - When IS Auditors believe that **bank has accepted residual risk that is inappropriate for org.**, **discuss** same with appropriate level of management. If IS Auditors are not in agreement with decision, **report matter to BOD or AC.**


(rajveer.an.indian@gmail.com)

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUSES

**Requirements of SEBI for System Controls & Audit: SEBI** is regulator for securities market in India.

**System Audit:**

- SEBI mandated **annual system audit of SE by reputed independent auditor**.
- Conduct audit **as per Norms, Terms of References (TOR) & Guidelines issued by SEBI**.
- **Board** of SE/Depositories **can appoint Auditor. Auditor** can perform **maximum 3 successive audit**.
- **Audit schedule** to be submitted **to SEBI at-least 2 months in advance**, along **with scope of current audit & previous audit**.
- **Scope** of Audit may be **extended by SEBI considering changes** during last year / post previous audit report
- **Audit report be submitted to Auditee**. Report should have specific compliance/non-compliance issues, observations for minor deviations & qualitative comments for scope improvement.
- Report should also **take previous audit reports in consideration & cover any open items therein**.
- Auditee **management** must provide their **comment about Non-Conformities & observations**. **Corrective action** must be taken **within 3 months & reported to SEBI**.
- **Audit report along with Management Comments** shall be submitted **to SEBI within 1 month of completion of audit**.

**Audit Report Norms:**

- **Systems Audit Reports & Compliance Status** should be **placed before Governing Board** of SEs / Depositories & system audit report along **with comments** of SEs / Depositories should be **communicated to SEBI**.
- **Audit report** should have **explicit coverage of each Major Area mentioned in TOR,** indicating any **Nonconformity** (NCs) or **Observations** (or lack of it). For each section, auditors should also provide qualitative input about ways to improve process, based upon best practices observed.

**Auditor Selection Norms**

- Auditor must have **minimum 3 years of experience in IT audit** of Securities Industry participants e.g. SE, clearing houses, depositories etc.
- Auditor must possess **recognized certification** like CISA.
- Auditor must **not have any conflict of interest** in conducting fair, objective & independent audit of Exchange/Depository.
- Auditor should **not** have been **engaged over last 3 years** in any **consulting engagement** with any dept./units of entity being audited.
- Auditor must **not have** any **cases pending** against its **previous auditees**.

**System Controls:**

- SE/Depositories to submit **declaration from MD/CEO certifying security & integrity of** their **IT Systems** along **with Audit report**.
- **Proper audit trail for upload / modifications / downloads of KYC data** to be maintained.

## CYBER FORENSIC & CYBER FRAUD INVESTIGATION

- Cyber forensics is one of **latest scientific techniques**, **emerged due to effect of increasing computer frauds**.
- **Cyber** - 'The Net' i.e. online. **Forensics** - Scientific method of investigation & analysis techniques to gather, process, interpret, & to use evidence to provide conclusive description of activities in suitable way for presentation in court of law. **Cyber Investigation - Investigation method to gather digital evidences to produce in court of law**.
- **Cyber forensic experts follow standard & globally accepted methods for investigation** so that same result shall always be obtained if same evidences are checked by another expert.
- Increasing frauds across cyber space has surprised law keeper's. **Fraudsters always look to misuse any loop hole / weaknesses** in computer systems. Cyber Frauds withdrawal of USD45 Million by using ATM cards sent shock waves across IT security agencies.
- There is **increasing demand for experts in field of cyber forensics**.
- IT Act u/s **43A & sec - 65 to 67B lists various types of cyber-crimes & specifies penalty**.

## STANDARD ON AUDITING (SA) 402

Audit Considerations Relating to **Entity using Service Organization (SO)**. It deals with **user auditor's responsibility to obtain SAAE** when user entity uses services of one or more SO. SA 402 also deals with aspects like obtaining understanding of services provided by SO, including IC, responding to Assessed ROMM, Type 1 & Type 2 reports, fraud, non-compliance with laws & regulations & Uncorrected MS in relation to activities at SO & reporting by user auditor.



(rajveer.an.indian@gmail.com)

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUSES

## SECURITY STANDARDS

Information security is essential in day-to-day operations, breaches in information security can lead to substantial impact like reputational or legal risk, which can jeopardize customer or employee relations or endanger the survival of enterprise. COBIT 5 (published by ISACA) highlights needs for enterprises to ensure required level of security is implemented.

- Maintain information risk at an acceptable level & protect information against unauthorised disclosure / modifications or possible intrusions;
- Ensure that services & systems are continuously available;
- Comply with laws & regulations, contractual requirements & internal policies.; and
- Achieve all above & at same time controlling cost of IT services & technology protection.

**NATIONAL CYBER SECURITY POLICY 2013**

**Vision - "To build a secure & resilient** (flexible) **cyberspace for citizens, business & Government"**

**Mission - "To protect information & information infrastructure in cyberspace, build capabilities to prevent & respond to cyber threats, reduce vulnerabilities & minimize damage from cyber incidents through combination of institutional structures, people processes, technology & cooperation".**

To protect information infrastructure & CIA of information in cyberspace, it is essence to secure cyber space**. MAJOR OBJECTIVES OF THIS POLICY**:

- To **create a secure cyber ecosystem, generate adequate trust & confidence in IT systems & transactions** in cyberspace to enhance its adoption;
- To create an **assurance framework for design of security policies & for promotion & enabling actions for compliance with global security standards & best practices**;
- To **strengthen Regulatory framework** for ensuring Secure Cyberspace ecosystem;
- To enhance **protection & resilience of Nation's critical information infrastructure** by operating 24x7;
- To **improve visibility of integrity**;
- To create a **workforce of 500,000 professional skilled** in cyber security **in next 5 years** through capacity building, skill development & training;
- To protect information for **safeguarding privacy of citizen's data** & for **reducing economic losses** due to cybercrime / data theft;
- To enable **effective prevention, investigation & prosecution** of cybercrime & enhancements of law enforcement;
- To **enhance global cooperation**.

**ISO 27001**

Information security is not just about anti-virus software, implementing latest firewall or locking down laptops or web servers.

ISO/IEC 27001 (International Organization for Standardization / International Electro-technical Commission) defines **how to organize information security in ANY organization**. This standard is **foundation of Information Security Management** & **written by world's best experts** & aims to **provide a methodology for implementation of information security** in organization. It also **enables organization to get certified** (by independent certification body) that information security has been implemented in best possible way in organization.

**ISO/IEC 27001 formally specifies** an **INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS).** ISMS is a management framework through which organization **identifies, analyzes & addresses its information security risks**. It is a **systematic approach for managing confidential / sensitive information** so that it remains secure (i.e. maintaining **CIA**). It encompasses people, processes & IT systems & helps us to coordinate both electronic & physical security consistently & cost effectively.

**ISO/IEC 27001:2005 -** The Plan-Do-Check-Act (PDCA) cycle

ISO 27001 prescribes **ISMS**, which consists of **4 phases** that should be continuously implemented to minimize risk to CIA of information:

- **The Plan Phase (Establishing the ISMS) –** Plan basic organization of information security, set objectives, & choose appropriate security controls (Standard contains a catalogue of 133 possible controls).
- **The Do Phase (Implementing & Working of ISMS) –** Carry out everything that was planned in previous phase.
- **The Check Phase (Monitoring & Review of the ISMS) –** Monitor functioning of ISMS & check whether results meets set objectives.
- **The Act Phase (Update & Improvement of the ISMS) –** Improve everything that was identified as non-compliant in previous phase.

The cycle of these four phases never ends.

**ISO/IEC 27001:2013** is first revision of ISO/IEC 27001 that specifies requirements for **establishing, implementing, maintaining & continually improving an ISMS within context of organization.** Its requirements are generic & are intended to be applicable to all organizations, regardless of type/size/nature. It does not put so much emphasis on PDCA cycle.

**Structure**

The reason for elimination of PDCA cycle is that requirement is for continual improvement & PDCA is just one approach to meeting that requirement. There are other approaches, & organizations are now free to use them if they wish.

**Changes from the 2005 standard**

New standard puts more emphasis on measuring & evaluating how well an organization's ISMS is performing, & there is new section on outsourcing (many organizations rely on third parties to provide some aspects of IT). Major change is that it does not emphasize on PDCA cycle & other continuous improvement processes like Six Sigma's can be implemented.

**Benefits of ISO 27001**

- Can act as extension of current quality system to include security.
- Provides opportunity to identify & manage risks to key information & systems assets.
- Provides confidence & assurance to trading partners & clients, & acts as a marketing tool.
- Allows independent review & assurance on info. security practices.

**Reason to adopt ISO 27001:**

- Suitable for protecting critical & sensitive information.
- Provides a holistic, risk-based approach to secure information & compliance.
- Demonstrates credibility, trust, satisfaction & confidence with stakeholders, partners & customers.
- Demonstrates security status according to internationally accepted criteria.
- Creates market differentiation due to prestige, image & external goodwill.
- If company is certified once, it is accepted globally.



(rajveer.an.indian@gmail.com)

# CHAPTER – 7 INFORMATION TECHNOLOGY REGULATORY ISSUSES

## INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL)

ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with needs of business. It is published in SERIES OF FIVE CORE PUBLICATIONS, each of which covers an ITSM lifecycle stage. It allows org. to establish a baseline from which it can plan, implement, & measure. It is used to demonstrate compliance & to measure improvement. Although UK Government originally created ITIL, it has rapidly been adopted across world as standard for best practice in provision of IT services. ITIL V3 has transformed ITIL from providing a good service to being the most innovative & best in class. ITIL V3 has following **5 MODULE/STAGES**:

**Service Strategy:** Center & origin point of ITIL Service Lifecycle, it provides directions for other 4 stages & CLARIFY & PRIORITIZE SERVICE which the org. will offer & what capabilities need to be developed.

- **IT Service Generation:** ITSM refers to **implementation & management of quality IT services** & is performed by IT service providers through People, Process & IT.
- **Service Portfolio Management:** IT portfolio management is the **application of systematic management to investments, projects & activities** of enterprise IT departments.
- **Financial Management:** Its aim is **to give accurate & cost effective situation** of IT assets & resources used in providing IT Services.
- **Demand Management:** It is **planning methodology**, **use to manage & forecast demand** of products & services.
- **Business Relationship Management:** It is formal **approach to understand, define, & support broad range of inter -business activities** related to providing & consuming knowledge & services via networks i.e. IT.

**Service Design:** It translates strategic plans & objectives into DESIGNS & SPECIFICATIONS for execution through service transition & operations. It provides guidance on combining infrastructure, applications, systems, & processes, along with suppliers & partners, to provide best possible services.

- **Service Catalogue Management:** It maintains & produces Service Catalogue & ensures that it contains accurate details of all services made available to customers including ordering & requesting processes, prices, deliverables & contract points.
- **Service Level Management:** It provides for continual identification, monitoring & review of levels of IT services specified in Service-Level Agreements (SLAs).
- **Availability Management:** It ensures availability of services whenever needed, it addresses IT components abilities like reliability, maintainability, serviceability, resilience & security to perform at an agreed level.
- **Capacity Management:** It supports optimum & cost-effective provision of IT services by matching IT resources to business demands. Also helps in workload management; demand management; capacity planning; resource management & performance management etc.
- **IT Service Continuity Management:** ITSCM ensure that IT services can recover & continue even after a serious incident occurs.
- **Information Security Management:** Its goal is to ensure adequate information security to protect information assets against risks to maintain their value to the organization, i.e. ensuring their confidentiality, integrity & availability, along with authenticity, accountability, non-repudiation & reliability.
- **Supplier Management:** Its purpose is to obtain value for money from suppliers & contracts.

**Service Transition:** This is where org. BUILD, TEST & IMPLEMENT THEIR NEW SERVICE DESIGNS. By following these steps & rectifying issues that arise, it can ensure effectiveness of its operation & maintenance, prevention of undesired consequences / failure / disruption of their service.

- **Service Transition Planning & Support:** It ensures orderly transition of new / modified service into production with necessary adaptations.
- **Change management & Evaluation:** It ensures that standardized methods & procedures are used for efficient handling of all changes.
- **Service Asset & Configuration Management:** It focuses on maintaining information (i.e. configurations) about Configuration Items (i.e. assets) required to deliver IT service.
- **Release & Deployment Management:** It is used by software migration team as platform for software & hardware including controls across the entire IT infrastructure to ensure its functions as intended when introduced into existing infrastructure or live environment.
- **Service Validation & Testing:** It ensures that released & deployed services meet customer expectations & IT operations are able to support new services.
- **Knowledge Management:** It is process of capturing, developing, sharing & effectively using organisational knowledge to organisational objectives.

**Service Operation:** After service have been validated, they are put into live environment. Even though org. would have corrected issues it encountered but new ones will arise when customers start using the service. Service Operation provides guidance on MANAGEMENT OF SERVICE & SUPPORTING OPERATIONS (like shared services, web services, mobile commerce) ON DAY-TO-DAY BASIS.

- **Functions**: The major functions are:
  - **Service Desk**
  - **Application management**
  - **IT Operations**
  - **IT Technical Support**
- **Incident Management:** It aims to restore normal service operation as quickly as possible & minimize adverse effect on business operations to ensure.
- **Request fulfillment/Request management:** It focuses on fulfilling Service Requests like minor changes (e.g., requests to change password) or requests for info.
- **Access Management:** It grants authorized users to use service & prevents access of non-authorized users.
- **Event Management:** Event - indicate that something is not functioning correctly. Event management generates & detects notifications, while monitoring checks status of components even when no events are occurring.
- **Problem Management:** It aims to resolve root causes of incidents & minimize adverse impact of incidents caused by errors & its recurrence.

**Continual Service Improvement:** Org. should never be satisfied with the quality of their services, as there will always be snags & things that can be improved. It works with other 4 stages of service lifecycle to align business with business needs, whilst recognizing improvement, opportunity & changes.
It provides guidance on measurement of service performance through service life-cycle, suggest improvements to ensure that service delivers maximum benefit.


(rajveer.an.indian@gmail.com)

# CHAPTER – 8 EMERGING TECHNOLOGIES

**GRID COMPUTING:** In most organizations, computing resources are underutilized but are necessary for certain operations. The idea of Grid Computing is to make use of such non-utilized computing resources by needy organizations, & thereby ROI on computing investments can be increased.
Thus, **Grid Computing is network of computing or processor machines managed with a kind of software** such as **MIDDLEWARE, to access & use resources remotely**.
Grid Services requires use of software which can divide & carve out pieces of a program as one large system image to several thousand computers.

**Reason for popularity of Grid Computing**

- It can make use of unused computing resources, & thus, it is cost-effective solution (reducing investments, only recurring costs).
- Enables heterogeneous (dissimilar) resources of computers to work cooperatively & collaboratively to solve a scientific problem.

**CLOUD COMPUTING:** It means **use of computing resources as a service through networks**, say Internet. It **helps users to access database resources via Internet from anywhere at any time, without worrying about any maintenance or management of actual resources**. **E.g. Google Apps,** where any application can be accessed using a browser & can be deployed on thousands of computer through Internet.
It is **combination of software & hardware based computing resources delivered as a networked service**. These applications & resources can be accessed using a simple front-end interface such as Web browser from any client device like notebooks, desktops, mobile devices etc. The location of such physical resources & devices being accessed are generally not known to end users.
It helps companies to **scale upto massive capacities instantly** without having to invest in new infrastructure, train new personnel or license new software. Cloud computing is of **benefit to small & medium-sized business**, who wish to completely outsource their data-centre infrastructure; or **large companies**, who wish to get peak load capacity without incurring higher cost of building larger data centres. In both instances, service consumers use '**what they need on Internet**' & '**pay only for what they use'.**

**Cloud Computing Vs Grid Computing:** Cloud Computing evolved from grid computing & provides on-demand resources provisioning. Grid Computing require use of software that can divide & carve out pieces of program as one large system image to several computers. If one piece of software on a node fails, other piece of software on the other node also fails. There are some similarities & differences b/w these two.

**Similarities:**

- **Scalable:** Scalability is achieved through load balancing of application. CPU & network bandwidth is allocated & de-allocated on demand. The system's storage capacity goes up & down depending on number of users & amount of data transferred at a given time.
- **Both involve Multitenancy & Multitasking:** Many customers can perform different task accessing single or multiple application. Sharing resources among a large pool of users reduce infrastructure cost. Both provide Service-Level Agreements (SLAs) for guaranteed uptime availability (say 99%), consumer get service credit for not receiving data in guaranteed time.

**Differences:**

- Grid Computing is most **beneficial & economical when amount of distributed data is large**. While in cloud computing, we can store an object as **low as 1 byte & as large as 5 GB or even several TBs**.
- Grid computing **focuses on computationally intensive operations**, while cloud computing offers two types of services: **standard & high-CPU**.

**Pertinent Objectives to achieve goals of Cloud Computing / Goals of Cloud Computing:**

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

**Cloud Computing ARCHITECTURE:** It is structure of system & consists of **Front End** & **Back End**. They connect to each other through network (usually Internet). Front End is side, the computer user sees & interacts through, and Back End is the "cloud" section of system, truly facilitating services.

- **FRONT END ARCHITECTURE:** It comprises of client's devices (or computer network) & some applications needed for accessing the cloud computing system. All cloud computing systems do not give same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.
- **BACK END ARCHITECTURE:** Back end is cloud itself, which comprise of various computer machines, data storage systems & servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as online video games.

A **central server** is established for administering whole system. It also monitor client's demand as well as traffic to ensure that system is running without any problem. It follow some protocols & also uses a software known as middleware. **Middleware** helps computers on networks to communicate with each other.

**CLOUD COMPUTING ENVIRONMENT:** It can consist of multiple **TYPES OF CLOUDS** based on their deployment & usage.

- **PRIVATE CLOUD**
- **PUBLIC CLOUD**
- **COMMUNITY CLOUD**
- **HYBRID CLOUD**

# CHAPTER – 8 EMERGING TECHNOLOGIES

**Private Cloud:** This cloud computing environment resides within boundaries of org. & is used exclusively for organization's benefits. Also called Internal Clouds or Corporate Clouds. **Private Clouds can either be private to org. & managed by single org. (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud).** They are built primarily by IT departments within enterprises to optimize utilization of infrastructure resources within enterprise by using concepts of grid & virtualization.

**Characteristics of Private Cloud**

- **Secure:** As it is deployed & managed by org. itself, hence there is least chance of data being leaked,
- **Central Control:** As it is managed by org. itself, there is no need to rely on outsiders & it is controlled by org. itself,
- **Weak Service Level Agreements (SLAs):** SLAs play a very important role in any cloud service deployment model as they are defined as agreements b/w user & service provider. In private cloud, either Formal SLAs do not exist or are weak as it is b/w org. & user of same org.

**Advantages of Private Cloud**

- **Provides high level of security & privacy to user.**
- **Small in size & controlled & maintained by org.**

**Limitation:** Org. may have to invest in buying, building & managing clouds independently**. Budget is constraint in private clouds & also have loose SLAs.**

| | ON-PREMISE PRIVATE CLOUD | OUTSOURCED PRIVATE CLOUD |
|---|---|---|
| **Management** | Managed by org. itself. | Managed by third party. Everything is same as private cloud except that the cloud is outsourced. |
| **SLAs** | SLAs are defined b/w org. & its users, which is weak or may not exist. | These are usually followed strictly as it is a third party org. |
| **Network** | Network management & network issue resolving are easier. Networks usually have high bandwidth & low latency. | It is fully deployed at third party site & org. connect to third party by means of either a dedicated connection or through Internet. |
| **Security & Data Privacy** | It is more secure than any other cloud & security attacks are possible from internal user only. | It is relatively less secure & security threat is from third party & internal employee. |
| **Location** | Data is usually stored in same geographical location where cloud users are present. In case of several physical locations, cloud is distributed over several places & is accessed using Internet. | Cloud is located off site & when there is a change of location data need to be transmitted through long distances. |
| **Performance** | Performance depends on network & resources and can be controlled by internal IT dept. | Performance depends on third party who is outsourcing the cloud. |

**Public Cloud:** This environment can be used by general public includes individuals, corporations & other types of org. Typically, public clouds are administrated by third parties or vendors over Internet & services are offered on pay-per-use basis. These are also called Provider Clouds. **Public cloud consists of users from all over world wherein a user can simply purchase resources on an hourly basis & work with such resources which are available in cloud provider's premises.**

**Characteristics of Public Cloud:**

- **Highly Scalable:** Resources in public cloud are large in number & service providers make sure that all requests are granted.
- **Affordable:** Cloud is offered to public on pay-as-you-go basis; hence user has to pay only for what he is using (i.e. using on per-hour basis) which does not involve any cost of deployment.
- **Less Secure:** Since it is offered by third party & they have full control over cloud.
- **Highly Available:** Because anybody from any part of world can access public cloud with proper permission which is not possible in other models as there might be geographical or other restrictions.
- **Stringent SLAs:** As cloud provider's business reputation & customer strength are totally dependent on cloud services, they follow SLAs strictly & violations are avoided.

**Advantages of Public Cloud**:

- Widely used in development, deployment & management of enterprise applications, at affordable costs.
- Allows org. to deliver highly scalable & reliable applications at more affordable costs.
- No need of establishing infrastructure for setting up & maintaining cloud.
- **Strict SLAs are followed.**
- **No limit for number of users.**

**Limitations:** Security assurance & thereby building trust among clients is difficult. **Privacy & organizational autonomy are not possible.**

**Hybrid Cloud:** This is combination of both at least one private (internal) & at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms & applications. **Usual method of using hybrid cloud is to have a private cloud initially & then for additional resources, public cloud is used. Hybrid cloud is private cloud extended to public cloud & aims at utilizing power of public cloud by retaining properties of private cloud.** It is typically offered in either of 2 ways.

1. A vendor has private cloud & forms partnership with public cloud provider or
2. A public cloud provider forms partnership / franchise with vendor providing private cloud platforms.

**Characteristics of Hybrid Cloud**:

- **Scalable:** Hybrid cloud has property of public cloud with private cloud environment & as public cloud is scalable; hybrid cloud is also scalable.
- **Partially Secure:** Private cloud is secured & public cloud has high risk of security breach. Hybrid cloud cannot be fully termed as secure but as partially secure.
- **Stringent SLAs:** SLAs are stricter than private cloud & might be as per public cloud service providers.
- **Complex Cloud Management:** As it involves more than 1 type of deployment models & also number of users is high.

**Advantages of Hybrid Cloud:**

- **Highly scalable & gives power of both private & public clouds.**
- **It provides better security than public cloud.**

**Limitation: Security features are not as good as private cloud & complex to manage.**

# CHAPTER – 8 EMERGING TECHNOLOGIES

**Community Cloud: It is cloud infrastructure which is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns. It may be owned, managed & operated by one or more organizations in community, a third party or combination of them, and it may exist on or off premises. In this, a private cloud is shared b/w several organizations. This model is suitable for org. which cannot afford private cloud & cannot rely on public cloud either.**

**Characteristics of Community Clouds:**

- **Collaborative & Distributive Maintenance:** In this, no single company has full control over whole cloud. This is usually distributive & hence better cooperation provides better results.
- **Partially Secure:** Few organizations share the cloud, so there is a possibility that data can be leaked from one org. to another, though it is safe from external world.
- **Cost Effective:** As complete cloud is shared by several organizations or community, hence it becomes cost effective.

**Advantages of Community Clouds:**

- **Allows establishing a low-cost private cloud.**
- **Allows collaborative work on cloud.**
- **Allows sharing of responsibilities among organizations.**
- **Better security than public cloud.**

**Limitation: Autonomy of org. is lost & security features are not good as private cloud. It is not suitable in cases of no collaboration.**

**CLOUD COMPUTING SERVICE MODELS: Cloud computing is model which enables end users to access the shared pool of resources such as compute, network, storage, database & application as an on- demand service without need to buy or own it. The services are provided & managed by service provider, reducing management effort from end user side. The essential characteristics of cloud include on-demand, self-service, broad network access, resource pooling, rapid elasticity, and measured service.**

| IaaS | | | | | Paas | SaaS | | | Other | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| NaaS | STaaS | DBaaS | BaaS | DTaaS | | TaaS | APIaaS | EaaS | CaaS | DaaS | SECaaS | IDaaS |

**Infrastructure as a Service (IaaS):**

- **IaaS, a hardware-level service, provides computing resources like processing power, memory, storage & networks for cloud users to run their application on-demand.**
- **This allows users to maximize utilization of computing capacities without having to own & manage their own resources.**
- **IaaS changes computing from physical infrastructure to virtual infrastructure through virtual computing; storage; network resources by removing physical resources.**
- In order to deploy their applications, cloud clients install OS images & their application software on cloud infrastructure.
- E.g. Amazon Web Services (AWS).

**A typical IaaS provider may provide following services (i.e. SERVICES BY IaaS):**

- **Compute: Computing as a Service includes virtual CPUs & virtual main memory for Virtual Machines (VMs) which are provisioned to end users.**
- **Storage: STaaS provides back-end storage for VM images. Some of IaaS providers also provide back end for storing files.**
- **Network: NaaS provides virtual networking components such as virtual router, switch & bridge for VMs.**
- **Load Balancers: Load balancing as a Service may provide load balancing capability at infrastructure layer.**

**Characteristics of IaaS:**

- **Web access to resources: IaaS model enables IT users to access infrastructure resources over Internet. IT user need not to get physical access to servers while accessing a huge computing power.**
- **Centralized management: Distributed resources can be easily controlled by management support which ensures effective resource management & utilization.**
- **Elasticity & Dynamic Scaling: Depending on load, resources can be increased or decreased according to the requirements.**
- **Shared infrastructure: IaaS follows one-to-many delivery model & allows multiple IT users to share same physical infrastructure which ensure high resource utilization.**
- **Metered Services: IaaS allows IT users to rent computing resources instead of buying it. IT users will be charged as per amount of usage & consumption of services.**

| **Network as a Service (NaaS):** | **Storage as a Service (STaaS):** | **Database as a Service (DBaaS):** | **Backend as a Service (BaaS):** | **Desktop as a Service (DTaaS):** |
|---|---|---|---|---|
| NaaS, an instance of IaaS, provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. End-users can access virtual network services provided by service provider over Internet on pay-per-use basis. E.g. VPN. | STaaS, an instance of IaaS, provides storage infrastructure on subscription basis to users who want a low-cost & convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery & preserve records for long-term. The end users can store data on virtual storage provided by service provider & can access files at any time from any place. | This is also related to IaaS & provides users with seamless mechanisms to create, store & access databases at a host site on demand. The end users can access database service without need to install & maintain it on pay-per-use basis. | It is a type of IaaS, that provides web & mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration. | It is an instance of IaaS that provides ability to end users to use desktop virtualization without buying & managing their own infrastructure. DTaaS is pay-per-use cloud service delivery model in which service provider manages back-end responsibilities of data storage, backup, security & upgrades. The end-users are responsible for securing & managing their own desktop images, applications, & security. It is simple to deploy, highly secure & produce better experience. |

# CHAPTER – 8 EMERGING TECHNOLOGIES

**Platform as a Service (PaaS):**

- **PaaS provides users the ability to develop & deploy an application on development platform provided by service provider.**
- **In traditional application development, the application will be developed locally & will be hosted in central location. PaaS changes the application development from local machine to online. E.g. Google AppEngine, Windows Azure Compute etc.**

**A typical PaaS provider may provide following (i.e. SERVICES BY PaaS):**

- **Programming Languages: PaaS providers provide a wide variety of programming languages (E.g. Java, PHP) for developers to develop applications.**
- **Application Frameworks: PaaS vendors provide application development framework for application development.**
- **Database: Along with PaaS platforms, PaaS providers provide some databases so that application can communicate with the databases.**
- **Other Tools: PaaS providers provide all the tools that are required to develop, test & deploy an application.**

**Characteristics of PaaS:**

- **All in One: Most of PaaS providers offer services like programming languages to develop, test, deploy, host & maintain applications in the same Integrated Development Environment (IDE).**
- **Web access to development platform: PaaS provides web access to development platform which helps developers to create, modify, test & deploy different applications on same platform.**
- **Offline Access: To enable offline development, PaaS providers allow developer to synchronize their local IDE with PaaS services. The developers can develop an application locally & deploy it online whenever they are connected to Internet.**
- **Built-in Scalability: PaaS services provide built-in scalability to an application that is developed using any particular PaaS. It ensures that application is capable of handling varying loads efficiently.**
- **Collaborative Platform: To enable collaboration among developers, PaaS providers provide tools for project planning & communication.**
- **Diverse Client Tools: PaaS providers offer a wide variety of client tools like Web User Interface (UI) & Application Program Interface (API) to help developers to choose tools of their choice.**

**Software as a Service (SaaS):**

- **SaaS provides ability to end users to access an application over Internet which is hosted & managed by service provider. Thus, end users are exempted from managing or controlling an application. SaaS changes the way the software is delivered to customers.**
- **In traditional software model, software is delivered as a license-based product which need to be installed in end user device. SaaS is delivered as an on-demand service over the Internet, there is no need to install the software in end-user's devices. SaaS services can be accessed or disconnected at any time based on the end user's needs.** E.g. Google Docs & online photo editor.

**Services provided by SaaS:**

- **Business Services: SaaS providers provide a variety of business services to startup companies E.g. ERP, CRM, billing, sales & human resources.**
- **Social Networks: Since number of users of social networking sites is increasing exponentially, loud computing is perfect match for handling variable load.**
- **Document Management: SaaS providers provide services to create, manage & track electronic documents as most of enterprise extensively use electronic documents.**
- **Mail Services: To handle unpredictable number of users & load on e- mail services, most of email providers offer their services as SaaS services.**

**Characteristics of SaaS:**

- **One to Many: SaaS services are delivered as one-to-many models where a single instance of application can be shared by multiple customers.**
- **Web Access: End users can access application from any location via device is connected to Internet.**
- **Centralized Management: Since SaaS services are hosted & managed from central location, SaaS providers perform automatic updates to ensure that each customer is accessing most recent version of application without any user-side updates.**
- **Multi-device Support: SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smartphones etc.**
- **Better Scalability: Most of SaaS services leverage PaaS & IaaS for its development & deployment and ensure a better scalability than traditional software.**
- **High Availability: SaaS services ensure 99.99% availability of user data as proper backup & recovery mechanisms are implemented.**
- **API Integration: SaaS services have the capability of integrating with other software or service through standard APIs.**

| | | |
|---|---|---|
| **API as a Service (APIaaS):** This allows users to explore functionality of Web services such as Google Maps, Payroll processing & credit card processing services etc. | **Testing as a Service (TaaS):** This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases & test result evaluation on a pay-per-use basis. | **Email as a Service (EaaS):** This provides users with an integrated system of emailing, office automation, records management, migration & emails archiving, spam blocking, malware protection & compliance features. |

# CHAPTER – 8 EMERGING TECHNOLOGIES

**Other Cloud Service Models**

**Communication as a Service (CaaS):**

- CaaS has evolved in the same lines as SaaS.
- CaaS is outsourced enterprise communication solution which can be leased from single vender.
- CaaS vendor is responsible for all hardware & software management & offers guaranteed Quality of Service (QoS).
- It allows businesses to selectively deploy communication devices on pay-as-you-go or need basis which eliminates large investments.
- E.g. VolP, Videoconferencing.

**Data as a Service (DaaS):**

- DaaS provides data on demand to users, systems or application.
- Data may include text, images, sounds & videos.
- Data encryption & OS authentication are commonly provided for security.
- DaaS users have access to high-quality data in centralized place & pay by volume or data type, as needed.
- As data is owned by providers, users can only perform read operations on data.
- E.g. Geography data or financial data services.

**Security as a Service (SECaaS):**

- End user can access security service provided by service provider on pay-per-use basis.
- Cloud security is moved into cloud itself whereby cloud service users will be protected from within the cloud.
- E.g. Email filtering, Web content filtering, Vulnerability management & Identity management.

**Identity as a Service (IDaaS):**

- End users (org. or enterprise) can access authentication infrastructure which is built, hosted, managed & provided by third party service provider.
- E.g. Directory services
  Authentication services
  Risk & event monitoring
  Single sign-on services &
  Identity & profile management.

## CHARACTERISTICS OF CLOUD COMPUTING

- **High Scalability:** It enable servicing of business requirements for larger audiences through high scalability.
- **Agility (Responsiveness):** It works in 'distributed mode' environment. It shares resources among users & tasks, which improves efficiency & agility (responsiveness).
- **High Availability & Reliability:** Availability of servers is supposed to be high & more reliable as the chances of infrastructure failure are minimal.
- **Multi-sharing:** Since it work in distributed & shared mode, multiple users & applications can work more efficiently with reduced cost by sharing common infrastructure.
- **Services in Pay-Per-Use Mode:** SLAs b/w provider & user must be defined while offering services in pay per use mode.
- **Virtualization:** It allows servers & storage devices to increasingly share & utilize applications.
- **Performance:** It is monitored, consistent & loosely coupled architectures are constructed using web services as the system interface.
- **Maintenance:** Cloud computing applications are easier, because they are not to be installed on each user's computer & can be accessed from different places.

## ADVANTAGES / BENEFITS OF CLOUD COMPUTING

- **Cost Efficiency:** It is most cost efficient method to use, maintain & upgrade. Traditional desktop software costs companies a lot in terms of finance. It is available at much cheaper rates which significantly lowers the company's IT expenses. There are many one-time-payments, pay-as-you-go & other scalable options available, which make cloud very reasonable for company.
- **Almost Unlimited Storage:** It gives us almost unlimited storage capacity & one need not to worry about running out of storage space or increasing current storage space availability.
- **Backup & Recovery:** Since data is stored in cloud, backing it up & restoring same is relatively easier than storing same on physical device. Cloud service providers are competent enough to handle recovery of information which makes entire process of backup & recovery much simpler.
- **Automatic Software Integration:** Software integration occurs automatically. We do not need to take additional efforts to customize & integrate applications as per our preferences. It allows us to customize the options with great ease as per our suitability.
- **Easy Access to Information:** Once registered in cloud, one can access information from anywhere at any time via Internet. It let one move beyond time zone & geographic location issues.
- **Quick Deployment:** Entire system can be fully functional in a matter of few minutes. Of course, amount of time taken here will depend on exact kind of technology that we need for business.

**Security and Implementation Issues relating to Cloud Computing**

**Security Issues (CHALLENGES TO CLOUD COMPUTING):**

- **Confidentiality: Prevention of unauthorized disclosure of data is referred as Confidentiality**. Cloud works on public networks, there is requirement to keep data confidential **by use of encryption & physical isolation.**
- **Integrity: It refers to prevention of unauthorized modification of data & ensures that data is of high quality, correct, consistent & accessible.** Data should not be changed, tampered or deleted after being moved to cloud.
- **Availability: It refers to prevention of unauthorized withholding of data & ensures data backup through BCP & DRP.** Availability can be affected temporarily or permanently & a loss can be partial or complete e.g. temporary breakdown, Denial of services, equipment failure & natural calamities.
- **Governance: Due to lack of control over employees & services, there is problem relating to design, implementation, testing & deployment. So, there is need of governance model, which controls standards, procedures & policies of organization.**

**Implementation/Adaptation Issues (PERTINENT ISSUES):**

- **Threshold Policy:** It is important to check threshold policy in a pilot study to test if program is workable before moving the program to production environment. It checks how the policy detect sudden increases in demand & also determine how unused resources are to be de-allocated & turned over to other work.
- **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, company may find it difficult to shift to another computing vendor having different formats for importing & exporting data. This may need to reformat / reorganize data or change the logic in applications.
- **Hidden Costs:** Cloud computing service providers do not reveal 'what hidden costs are'. E.g. Higher network charges. This outweighs

- **Trust:** Organization has direct control over security aspects & have responsibility to protect IS from risk. Cloud has still failed to build trust b/w client & service provider. **Trust ensures that service arrangements have sufficient means to manage security & privacy controls employed by Cloud provider.**
- **Legal Issues & Compliance: There are various types of laws & regulations vary from place to place, which impose security & privacy duties on organization.** It is responsibility of cloud suppliers to protect data & supply it to customer in secure & legal way.
- **Privacy: Privacy issues are embedded in each phase of Cloud design to decrease privacy risk.**
- **Audit: It is checking that 'what is happening in Cloud environment'.**
- **Data Stealing: Some Cloud providers do not use their own server, instead use server from other service providers which may be less secure & prone to loss from external server.**
- **Architecture: In architecture of Cloud computing models, there should be a control over security & privacy of system. Architecture of Cloud is based on a specific service model. Its reliable & secure infrastructure is dependent on design & implementation to support overall framework.**
- **Identity Management & Access control: Robust federated identity management architecture & internal strategy in org. provides a trust & ensures protection against attackers.** Using Cloud-based "Identity as a Service" may be a useful tool for outsourcing some identity management capabilities & facilitating federated identity management with Cloud providers.
- **Incident Response: It ensures to meet requirements of org. during & after incident of data crises.**
- **Software Isolation: To understand virtualization & other logical isolation techniques which Cloud provider employs in its multi-tenant software architecture & evaluate risks required for org.**
- **Application Security: Security issues occur when application moves to cloud platform. Service provider should have complete access to server with all rights for purpose of monitoring & maintenance of server.** Infected applications need to be monitored & recovered by Cloud security drivers.

costs they (Cloud SP) could save on new infrastructure, training new personnel, or licensing new software.

- **Unexpected Behavior:** Sometimes application works well at our company's internal data centre but may behave in unexpected manner in pilot study. In this case, we need to fix the problem before executing or obtaining services from cloud.
- **Security Issues:** Instead of waiting for an outage to occur, consumers himself should do security testing by checking how well vendor can recover data in case of data loss by asking for old stored data & check how long it takes to recover & verify whether such data matches with original data.
  Test a trusted algorithm to encrypt data on local computer & then try to access data on remote server in cloud using the decryption keys. If we can't read data, means decryption keys are corrupted, or vendor is using its own encryption algorithm.
- **Software Development in Cloud:** To develop software using high-end databases, the most likely choice is to use cloud server pools at internal data corporate centre & extend resources temporarily for testing purposes. It helps to control costs, manage security & allocate resources for a project.
- **Environment Friendly Cloud Computing:** Cloud computing is more environment friendly. It reduces no. of hardware components needed to run applications on company's internal data centre & replacing them with cloud computing systems which reduces energy requirement for running & cooling hardware. By consolidating these systems in remote centers, they can be handled more efficiently as a group.

**MOBILE COMPUTING:** It refers to technology that allows transmission of data via a computer without having to be connected to a fixed physical link (i.e. whereby users can connect to the network from anywhere, anytime & operate as if they were sitting in "home" office). Mobile voice communication is widely established throughout world & has had very rapid increase in no. of subscribers to cellular networks over last few years. An extension of this technology is the ability to send & receive data across these cellular networks. Mobile data communication has become very important & rapidly evolving technology, as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution of biggest problem of business people on move i.e. mobility.

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

**Components of Mobile Computing**

- **Mobile Communication: It refers to infrastructure put in place to ensure that seamless & reliable communication goes on. This would include communication properties, protocols, data formats & concrete technologies.**
- **Mobile Hardware: This includes mobile devices or device components which receive or access the service of mobility. E.g. Portable laptops, Smart Phones, Tablet PCs, PDA that use an existing & established network to operate on.**
  **At the back end, there are various servers like Application Servers, Database Servers, communication servers, etc.**
- **Mobile Software: It is actual programme that runs on mobile hardware & deals with characteristics & requirements of mobile applications. It is OS of that appliance & is essential component which makes mobile device operates. Mobile applications popularly called Apps, being developed by organizations for use by customers but these apps could represent risks like introduction of malware, access to personal information of mobile owner, etc.**

**How Mobile Computing Works?**

- **User enters or access data using application on handheld computing device.**
- **Using one of several connecting technologies, new data are transmitted from handheld to site's IS where files are updated & new data are accessible.**
- **Now both systems (handheld & site's computer) have same info. & are in sync.**
- **Process work the same way starting from other direction.**

**The process is similar to way a worker's desktop PC access organization's applications, except that user's device is not physically connected to organization's system.**

# CHAPTER – 8 EMERGING TECHNOLOGIES

**Benefits of Mobile Computing**

- It increases information quality & accessibility, enhances operational efficiency & improves management effectiveness.
- It provides mobile workforce with remote access to work order details, such as work order location, contact information, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time & facilitate excellent communication.
- It facilitates access to corporate services & information at any time, from anywhere.
- It provides remote access to corporate Knowledgebase at job location.
- It enhance information quality, information flow & ability to control mobile workforce which improves management effectiveness.

**Limitations of Mobile Computing**

- **Insufficient Bandwidth**: Mobile Internet access is generally slower than direct cable connections such as GPRS/EDGE, 3G & 4G networks. These networks are usually available within range of commercial cell phone towers. High speed wireless LANs are inexpensive but have very limited range.
- **Security Standards:** Working mobile requires careful use of VPN, since one is dependent on public *networks*.
- **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Due to compact size of devices, it requires expensive batteries to provide necessary battery life.
- **Transmission interferences:** Weather, terrain & range can interfere with signal reception. Reception in tunnels, some buildings & rural areas is often poor.
- **Potential health hazards:** People who use mobile devices while driving are more likely involved in traffic accidents. Cell phones may interfere with sensitive medical devices. Cell phone signals may cause health problems.
- **Human interface with device:** Screens & keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

**Issues in Mobile Computing**

- **Security Issues: Wireless networks require more security requirements than wired network. A number of approaches have been suggested say encryption.**
  - **Confidentiality: Preventing unauthorized users from gaining access to critical information of any particular user.**
  - **Integrity: Ensures unauthorized modification, destruction or creation of information cannot take place.**
  - **Availability: Ensuring authorized users getting the access they require.**
  - **Legitimate: Ensuring that only authorized users have access to services.**
  - **Accountability: Ensuring that users are held responsible for their security related activities.**
- **Bandwidth:** Bandwidth utilization can be improved by logging (bulk operations against short requests) & compression of data before transmission. Technique of caching frequently accessed data items can be used, cached data reduce query response time & also support during disconnected operations.
- **Location Intelligence:** In mobile computing; as computers are working in cells (mobile) & are being serviced by different network providers, a small movement may result in disconnection or disruption, if cell or network boundaries are crossed. Service connections must be dynamically transferred to nearest server.
- **Power Consumption:** Mobile Computers rely on their batteries as primary power source. Batteries should be light & should be capable of longer operation times. Power consumption should be minimized to increase battery life. Chips can be redesigned to operate at lower voltages. Individual Components, be powered down when they are idle.
- **Revising technical architecture:** Mobile users are demanding & are important to business world. To provide complete connectivity among users; current communication technology must be revised to incorporate mobile connectivity.
- **Reliability, coverage, capacity & cost:** Wireless network is less reliable, have less geographic coverage & reduced bandwidth, are slower & cost more than wired-line network services. It is important to find ways to use this new resource more efficiently by designing innovative applications.
- **Integration with legacy mainframe & emerging client/server applications:** As a result of the IT industry's original focus on mainframes, a huge inventory of applications using communications interfaces are incompatible with mobile connectivity. Still application development trend is geared towards wired network.
- **End-to-end design & performance:** Since mobile computing involves multiple networks (including wired) & multiple application server platforms; end-to-end technical compatibility, server capacity design & network response time estimates are difficult to achieve.
- **Business challenges:** In addition to technical challenges, mobile computing also faces business challenges due to lack of trained professionals.

**GREEN COMPUTING**

Green IT refers to study & practice of establishing / using Computers & IT resources in more efficient & environmental friendly & in responsible way. Computers consumes lot of natural resources in manufacturing, use power to run & problem of disposing them at end of their life cycle. This can include designing, manufacturing, using & disposing of computers, servers & associated subsystems peripheral devices efficiently & effectively with minimal or no impact on environment. The objective of green computing is to reduce use of hazardous materials, maximize energy efficiency & promote recyclability or biodegradability of defunct products & factory waste. Many corporate IT departments have taken Green Computing initiatives to reduce environmental impacts of their IT operations & things are evolving slowly but not as a revolutionary phenomenon.

All businesses are increasingly dependent on technology & small business is no exception. We work on our PCs, notebooks & smart phones all day, connected to servers running 24x7. These devices quickly become obsolete & we dispose of old devices & replace them with new ones. We use massive quantities of paper & ink to print doc, many of which we promptly send to circular file.

# CHAPTER – 8 EMERGING TECHNOLOGIES

**Green Computing Best Practices (STEPS FOR GREEN IT)**

The work habits of computer users & businesses can be modified to minimize adverse impact on global environment.

**Develop a sustainable Green Computing plan**

- Involve stakeholders to include recycling policies, recommendations for disposal of used equipment, government guidelines & recommendations for purchasing green computer equipment in organizational policies & plans;
- Encourage IT community for using best practices & encourage them to consider green computing practices & guidelines.
- Include power usage, reduction of paper consumption, recommendations for new equipment & recycling old machines in organizational policies & plans.
- Use cloud computing so that multiple organizations share same computing resources, which optimizes utilization of hardware resources.

**Recycle**

- Dispose e-waste according to central, state & local regulations;
- Discard used or unwanted electronic equipment in environmentally friendly manner as computers emit harmful emissions;
- Manufacturers must offer recycling options when products become unusable;
- Recycle computers through manufacturer's recycling services.

**Make environmentally sound purchase decisions**

- Purchase of desktop computers, notebooks & monitors which are less harmful to environment;
- Reducing packaging materials;
- Use Server & storage virtualization to improve resource utilization, reduce energy costs & simplify maintenance.

**Reduce Paper Consumption**

- Use of e-mail;
- Use of "track changes" feature in electronic doc., instead correcting on paper;
- Use online marketing instead paper based marketing; E.g. e-mail marketing.
- Print on both sides, use smaller fonts & margins, print required pages.

**Conserve Energy**

- Use LCD instead CRT monitors;
- Use notebook computers instead desktop;
- Use power-management features to turn off hard drives & displays after several minutes of inactivity;
- Power-down the CPU & all peripherals like printers during periods of inactivity;
- Use solar energy;
- Adapt Web conferencing instead of travelling to meetings & save energy.

**Green IT Security Services & Challenges**

IT solution providers are offering green security services in many ways. What to look in green security products, challenges in security services market.

- **Only if administered properly** with other green computing technologies, green security can be **cost-efficient & lucrative green IT service** for solution providers.
- Basic aim is to increase customer's energy savings through green security services & assess '**how sustainable computing technology can immediately help environment'**.
- Green IT services present many benefits for clients & providers, but **knowing 'how to evaluate client's infrastructure to accommodate green technology is a vital issue'**.

**BRING YOUR OWN DEVICE (BYOD):** It refers to business policy that allows employees to use their preferred computing devices, like smart phones & laptops for business purposes by connecting to corporate network to access information & application. BYOD policy has rendered the workspaces flexible, empowering employees to be mobile & giving them right to work beyond their required hours. It has led to increase in employees' satisfaction & also reduced IT desktop costs for organizations as employees are willing to buy, maintain & update devices in return for one-time investment cost to be paid by organization.

**Advantages of BYOD**

- **Happy Employees:** Employees love to use their own devices when at work. It also reduces no. of devices an employee has to carry; otherwise he would be carrying his personal as well as org. provided devices.
- **Lower IT budgets:** Employees could involve financial savings to org. since employees would be using devices they already possess which reduces outlay of org. in providing devices to them.
- **IT reduces support requirement:** IT department does not have to provide end user support & maintenance for all these devices resulting in cost savings.
- **Early adoption of new Technologies:** Employees are generally proactive in adoption of new technologies which results in enhanced productivity of employees leading to overall growth of business.
- **Increased employee efficiency:** Efficiency of employees is more when employee works on their own device. In an org. provided devices, employees have to learn.

**Emerging BYOD Threats**

Every business decision is accompanied with a set of threats & so is BYOD program too; it is not immune from them. A BYOD program that allows access to corporate network, emails, client data etc. is one of top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

- **Network Risks:** (Lack of Device Visibility) When company-owned devices are used by all employees within an organization, organization's IT practice has complete visibility of devices connected to network. This helps to analyze traffic & data exchanged over Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), IT practice team is unaware about no. of devices being connected to network & it can be hazardous. E.g. if virus hits network, all devices connected to network need to be scanned, it is probable that some devices would miss out such scan operation.
- **Device Risks:** (Loss of Devices) A lost or stolen device can result in enormous financial & reputational embarrassment to org. as device may hold sensitive corporate information.
- **Application Risks:** (Application Viruses & Malware) Majority of employees' phones & smart devices that were connected to corporate network weren't protected by security software. With increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security –organization or user'.
- **Implementation Risks:** (Weak BYOD Policy) Effective implementation of BYOD program should not only cover technical issues mentioned above but also mandate development of robust implementation policy. Because corporate knowledge & data are key assets of org. & in absence of strong BYOD policy may cause device misuse.

# CHAPTER – 8 EMERGING TECHNOLOGIES

**SOCIAL MEDIA**

A social network is usually created by a group of individuals, who have a set of common interests & objectives (say doctor). There are usually a set of network formulators followed by a broadcast to achieve network membership. This happens both in public & private groups depending upon confidentiality of network. After minimum numbers are met, network starts its basic operations & goes out to achieve its goal. Success of a social network mainly depends on contribution, interest & motivation of its members along with technology or platform support which makes life easier to communicate & exchange information to fulfill particular communication need.

**Web 2.0**

Web 2.0 is the term given to describe a second generation of World Wide Web that is focused on ability for people to collaborate & share information online. Two major technological advances enabled in Web 2.0 i.e. **Ajax & RSS**. Web 2.0 refers to transition from static HTML Web pages to a more dynamic Web that is more organized & is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with on Web-based communities of users, and more open sharing of information. **One of the most significant differences between Web 2.0 & traditional World Wide Web (referred as Web 1.0) is that Web 2.0 facilitates greater collaboration & information sharing among Internet users, content providers & enterprises. Thus it can be said that migration is from "read-only web" to "read-write web".**

**Components of Web 2.0 for Social Networks**

- **Communities:** These are online space formed by group of individuals to share their thoughts, ideas & have variety of tools to promote Social Networking in very easy & cost efficient manner.
- **RSS-generated Syndication:** It helps to syndicate web content which allows feed the freshly published web content to user through the RSS reader.
- **Blogging: Blog is a journal, diary, or a personal website that is maintained on internet & it is updated frequently by user by making post.** Blogs give freedom to express thoughts & help in generation & discussion of topics to user.
- **Wiki:** A Wiki is set of co-related pages on particular subject & allow users to share content. Wikis replace complex document management systems & are very easy to create & maintain.
- **Folksonomy: It allows users to classify & find information with the help of tagging. Also known as Social Bookmarking. Bookmarks are not stored on user's computer rather are stored on web increases accessibility from computer connected to Internet.**
- **Usage of Ajax: Ajax is a way of developing web application which combines XHTML & CSS.**
- **File Sharing/Podcasting:** It helps users to send their media files & related content online to other people on the network to see & contribute.
- **Mash-ups:** It helps to congregate services from multiple vendors to create a completely new service. E.g. combining location information from mobile service provider & map facility of Google maps to find exact information of cell phone device from internet, just by entering cell number.

**Types and Behavior of Social Networks** (based on needs and goals).

- **Social Contact Networks:** These types of networks are formed to keep contact with friends & family. E.g. Facebook, Instagram & Twitter.
- **Study Circles:** These are social networks for students, where they can have areas dedicated to student study topics, placement related queries & advanced research opportunity gathering. E.g. CA Club.
- **Social Networks for Specialist Groups:** These are specifically designed for core field workers like doctors, scientists, engineers, members of corporate industries. E.g. LinkedIn.
- **Networks for Fine Arts:** These social networks are dedicated to people linked with music, painting & related arts & have lots of useful networking information for all aspiring people of same line.
- **Police & Military Networks:** These networks operate like social networks on a private domain due to confidentiality of information.
- **Sporting Networks:** These social networks are dedicated to people of sporting community & have a range of information related to this field. E.g. Athlinks.
- **Mixed Networks:** There are number of social networks that have subscription of people from all above groups & is mixed social network serving multiple types of social collaboration.
- **Social Networks for 'inventors':** These social networks are for people who have invented concept of social networks, very developers & architects that have developed social networks. E.g. Technical Forums & Mash-up centres.
- **Shopping & Utility Service Networks:** Present world of huge consumerism has triggered people to invest in social networks, which will analyze social behaviour & send related information to respective marts & stores.
- **Others:** Apart from above, there are multiple other social networks, which serve huge number of internet population in multiple ways. Some of these networks die out very fast due to lack of constructive sustenance thoughts while others finally migrate to more specialist network.

**Life Cycle of Social Networks**

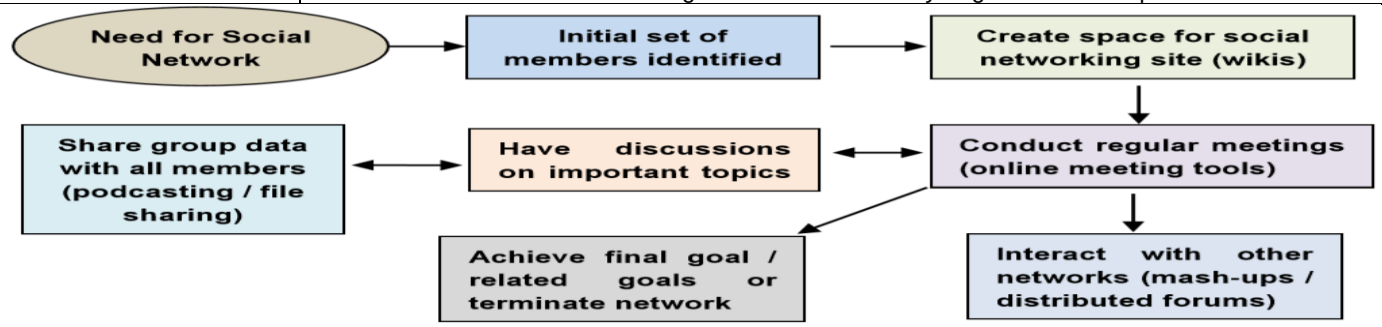
For any social network, there are no. of steps in its life cycle.

In each step, Web 2.0 concepts have a great influence.

For all steps, Web 2.0 provides tools & concepts, which are not only cost effective but very easy to implement.

Often, online networks have tendency to die out very fast due to lack of proper tools to communicate.

Web 2.0 provides excellent communication mechanism concepts like Blogging etc.



# CHAPTER – 8 EMERGING TECHNOLOGIES

**Application of Web 2.0**

Social networks built on Web 2.0 concepts has become so cost affordable & easy to use that more & more people are migrating to this wave. This has also helped NGO's & other social service org. to create social networks to reach out to people in much more structured manner (E.g. Community of Doctor). Web 2.0 finds applications in different fields:

- **Social Media: Social Media/Social Network provides a fundamental shift in the way people communicate & share information. It offers a no. of online tools & platforms that could be used by users to share their data, perspectives & opinions among other user communities.**
- **Marketing: Web 2.0 offers excellent opportunities for marketing by engaging customers in various stages of product development cycle. It allows marketers to collaborate with business partners & consumers on various aspects such as product development, service enhancement, and promotion. E.g. by Facebook.**
- **Education: Help students & faculty with more opportunities to interact & collaborate with their peers. By utilizing tools of Web 2.0, students gets opportunity to share what they learn with other peers by collaborating with them.**

**Benefits & Challenges for Social Networks using Web 2.0**

**Benefits**

- It provides a platform (social) where users of network need not to worry about implementation or underlying technology at affordable cost & easy pickup time.
- Concepts of Web 2.0 like blogging are some things that people do on day-to-day basis & no new knowledge skills are required.
- Web 2.0 techniques are very people centric activities & thus, adaptation is very fast.
- People are coming much closer to another and all social & geographical boundaries are being reduced at lightning speed.
- Using Web 2.0 also increases social collaboration to high degree & helps in achieving goals for social network.

**Challenges**

- One of major aspects is data security & privacy in such public domains, there is huge chance of data leak & confidentiality loss.
- Privacy of individual users can create huge problem if malicious users somehow manage to perpetuate social networks.
- Majority of social networks are offline & for bringing them online, lot of education & advertising needs to be done, which itself becomes cost burden especially when people involved are not computer literate.
- This becomes more difficult & requires huge efforts in areas of world that are developing & do not have basic amenities.

**Web 3.0**

- The term Web 3.0, also known as **Semantic Web**, describes sites **wherein computers will be generate raw data on their own without direct user interaction**.
- **Web 3.0 is considered as next logical step in evolution of Internet & Web technologies**.
- For **Web 1.0 & Web 2.0; Internet is confined within physical walls of computer**, but as more & more devices (such as smartphones, cars & other household appliances) become connected to web, **Internet will be omnipresent & could be utilized in most efficient manner**.

**Web 2.0 technologies allows use of read/write web**, **blogs, interactive web applications**, **tagging or folksonomy while sharing content & also social networking sites**. At same time, **Web 3.0 standard uses semantic web technology**, drag & drop mash-ups, widgets depending on interest & behaviour of individual users.

E.g. of Web 3.0 application is the one that **uses content management systems along with artificial intelligence**.

**Components of Web 3.0:**

- **Semantic Web: This provides web user a common framework that could be used to share & reuse data across various applications, enterprises, & community boundaries. This allows data & information to be readily intercepted by machines, so that machines are able to take contextual decisions on their own by finding, combining & acting upon relevant information on the web.**
- **Web Services: It is software system that supports computer-to-computer interaction over Internet. E.g. search of images via images on bing search.**

**To conclude, Web 3.0 helps to achieve a more connected open & intelligent web applications using concepts of natural language processing machine learning, machine reasoning & autonomous agents.**