Super Summary
Information Systems Control and Audit

Dedicated to all you guys.....

Chapter 1: Concept of Governance and Management of IS

Control requirement in Information System

- SEBI for listed companies in India
- Sarbanes Oxley Act of US
- Indian Company Act, 2013

Governance

All the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organised mechanism for evaluating options, setting direction, and monitoring compliance and performance, in order to satisfy specific enterprise objective.

(It constitutes the सम्पूर्ण accountability framework of a company क्योंकि it involves establishing accountability **for decision-making**)

Mechanism किस लिएं?

Enterprise Governance

The set of responsibilities and practices exercised by the board and executive management with the goal of

- Providing **strategic direction**,
- Ensuring that **objectives are achieved**,
- Ascertaining that **risks are managed properly**, and
- Verifying that organisation **resources are used responsibly.**

Corporate Governance (MT Nov, 2014)

The system by which a company is directed and controlled **to achieve the objective of increasing shareholder value** by enhancing economic performance.

IT Governance

What do you understand by IT Governance? Write any three benefits of IT Governance **(Nov, 14)**

Explain the key benefit of IT governance achieved at highest level in the enterprise.

The system by which IT activities in a company are directed and controlled **to achieve the business objectives** with the ultimate objective of meeting shareholders need.

Major Benefits of Governance

- **Achieving enterprise objective** by ensuring that each elements of mission and strategy are **assigned and managed** with the clearly understood and transparent **decision** right and responsibility; ;जब आपके पास कमबपेपवद लेने का तपहीज है then you will be held responsible for that decision outcome)
- **Defining and encouraging desirable behaviour** in the use of IT and in the execution of IT outsourcing arrangements;
- Implementing and integrating the **desired business process** into the enterprise;
- Providing **stability** and overcoming **limitation** of organisational structure;
- **Improving** customer, business and internal **relationships and satisfaction** and reducing internal territorial conflict by formerly integrating the customer, business units, and external IT providers into a complete IT governance framework; and
- Enable effective and strategically **aligned decision making** for the IT principles that define the role of IT, IT architecture, IT infrastructure, application portfolio and Framework, service portfolio, information and competency portfolio and IT investment and prioritisation. **(RTP-15M)**

Governance Dimensions (i.e. Aspects/Elements)

Conformance Dimension

It provides historic (significant) view and focuses on regulatory requirements.

This cover corporate governance issues (matter) such as: **Roles** of the chairman and CEO, **Role** and **composition** of the BOD, Board committee**, Controls Assurance** and **Risk Management Compliance**. Standard and regulation establishes all these aspects. Therefore, this aspect is auditable.

Performance Dimension

It is pro-active (practical) in its approach.

Business oriented and takes a forward looking view.

Focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand risk appetite and key performance drivers.

Not lend itself easily to a regime of standards and assurance as this specific to enterprise this is specific to enterprise goals and varies based on the mechanism to achieve them.

Benefit of IT Governance at the highest level

IT has to provide critical inputs to meet the information needs of all the stakeholders.' Define IT governance and list out its benefits. **(Nov, 15)**

- Increased **value delivered** through enterprise IT;
- Increased user **satisfaction** with IT services;
- Improved **agility** in supporting business needs;
- Best **cost performance** of IT;
- Improved **management and mitigation** of IT-related business risk;
- IT become an **enabler for change** rather than an inhibitor;
- Improved **transparency and understanding** of IT's contribution to the business;
- Improved **compliance with relevant** laws, regulation and policies; and
- more **optimal use** of IT resources.

IT steering committee function

Explain the key function of IT steering committee. **(MT-15M)**

- निश्चीत करना that long and short range **plans** of the IT department are **in tune with** enterprise goals and objective;
- स्थापित करना **size and scope** of IT function and **sets priorities** within the scope;
- To **review and approve** major IT deployment **projects** in all their stages;
- To approve and monitor **key projects** by measuring result of IT projects in terms of **return of investment**, etc;
- To **review** status of IS **plans and budgets** and overall IT **performance**;
- To review and approve standards, policies and procedures;
- To make **decisions** on all **key aspects** of IT deployment and implementation;
- To **facilitate** implementation **of IT security** within enterprise;
- To facilitate and resolve **conflicts in deployment** of IT and ensure availability of a viable communication system between IT and its users ; and
- To **report** to the BOD of IT activities on a regular basis.

Risk Assessment

Write short notes on Risk Assessment **(May, 13)**
Write short notes on Risk Assessment **(May, 14)**

A risk assessment activity can **provide an effective approach**, **which acts as the foundation for avoiding the disasters**. Risk assessment is also termed as **a critical step** in disaster and business continuity planning. Risk assessment is **necessary for developing** a well-tested contingency plan. In addition, Risk assessment is **the analysis of threats to resources** (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan.

Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritize applications, identify exposures and develop recovery scenarios.

Components **(VIT)**

(i) Impact Assessment,
(ii) Vulnerability Assessment, and
(iii) Threat Assessment.

Every entity **faces a variety of risks** from external and internal sources **that must be assessed.**

A precondition to risk assessment is the **establishment of objectives**, linked at different levels and internally consistent.

It is **the identification and analysis** of relevant risks **to achievement of the objectives**, forming **a basis** for determining how the risks should be managed.

Because economic, industry, regulatory and operating conditions will **continue to change**, mechanisms are needed to identify and deal with the special risks associated with change.

It is assessment **of the disruption** to critical activities, **which** are supported by resources such as PPTISS. The enterprise should determine the threat and vulnerability of each resource, and the impact which would have on, in case it becomes reality.

Risk Management

Risk is the possibility (सम्भावान) of something adverse happening, resulting in potential loss. These risks cannot be eliminated **but can be mitigated** by appropriate security.

RM is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.

It involves identifying, measuring and minimising **uncertain event** affecting **resources**. Because, vital activities in an enterprise are supported by these resources.
Any information system of which Information Technology is a subsystem has **inherent risk**.

Related terms

Asset: Something of value to the organisation. Organisation के लिए कोई वस्तु जो मुल्यवान है.
All assets have one or more of the following characteristics:

- Recognised to be of value to the organisation.
- Not easily replaceable without cost, skill, time, or resource. **(RTP-15M).**

Vulnerability: It is the Weakness in the system safeguard जो system को expose करता है threat के लिए. It may be कमजोरी in information system/cryptography system, that could be exploited (शोसन) by a threat.
Vulnerability must have at least one of the followings conditions;

- Allow an executor to execute command like another users' or
- Allows an attacker to access data that is contrary to the specified access restriction for that data or
- Allows an attacker to pose like another entity or
- Allows an attacker to conduct a DOS. **(May, 15) (Nov, 14) Q7**

Threat: Any entity, circumstance, or event with the potential (सम्भावना के साथ) to harm the system through (के जरिए) its unauthorised access, destruction, modification, and/or DOS is called threat.
Threat has capability (क्षमता) to attack (आक्रमन करने का) on a system with the intention to harm (नुकसान करने के इरादे के साथ). कोइ भी चीज जो **अनाधिकृत हो रहा** है ऊसी को threat कहते है जैसे **अनाधिकृत प्रवेश** destruction, modification etc **(RTP-15M). (Nov, 14)**

खतरा किसे कहते है? (Threat)
हानिकारक परिणामों की संभावना अथवा अपेक्षित हानि ही खतरा है।क

Exposure: It is the extent of loss organisation has to face when risk materializes.

Attack: It is an attempt (प्रयास) to gain unauthorised access to the system service or to compromise system dependability.

Risk: The potential harm (सम्भवीत नुकसान) can be caused if a particular **threat** exploits a particular **vulnerability** to cause damage to an asset.

Risk का मतलब सम्भवीत नुकसान हो जाना यदि एक threat, asset के किसी कमजोरी का शोसन करता है ऊस asset को क्षति/नुकसान पहुचाने के लिए। **(Nov, 14) Q7**

संकट किसे कहते है? (Risk)
प्राकृतिक या मानव प्रेरित वह खतरनाक घटना जिससे चोट **लग सकती है**, जीवन नष्ट **हो सकती है** या संपति, आजीविका और पर्यावरण को क्षति **हो सकती है।** संकट कहलाता है।

Countermeasure: An action, device, procedure, technique, or other measure that reduces the vulnerability of a system is called countermeasure. कोई पद्धति जिसके जरीए asset कि कमजोरी को कम किया जा सके.

Residual Risk: Any risk still remaining after the countermeasures are analysed and implemented is called residual risk. जैसा कि हम जानते हैं कोई भी risk को eliminate नहीं किया जा सकता है केवल risk reduce हो सकता है.

Risk Management Strategy (RTP 14N)

जब Risk Identified and Analysed हो जाता है तो यह हमेशा appropriate नहीं है कि control implement करें to counter them. Some risks may be minor, and it may not be effective to implement expensive control processes for them. RM is explained and illustrated below.

- **Tolerate/Accept the risk** बरदाश्ता करना: Management का एक मुख्य कार्य है कि risk manage करे, कुछ risk minor होते हैं because their impact & probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing risk to ensure its impact remains low.
- **Terminate/Eliminate the risk** समाप्ता करना : यह सम्भव है कि एक risk किसी technology use, supplier or vendor के साथ जुडा हो the risk can be eliminated by replacing technology with more robust technology and by seeking more capable supplier and vendor.
- **Transfer/Share the risk** साझा करना: Risk mitigation approach को हम share कर सकते हैं trading partner and supplier के साथ. Risk also may be mitigated by transferring the cost of realised risk to an insurance provider.
- **Treat/mitigate the risk** इलाज करना: जहॉ उपर के एक भी विक्लप नहीं लग पाता है तो suitable control must be devised and implemented to prevent the risk from manifesting itself or to minimise its effect.
- **Turn back**: Where the probability or impact of risk is very low, then management may decide to ignore the risk.

What do you understand by GEIT? Also explain its key benefits.

Governance Enterprise IT is a sub-set of corporate governance and facilitate implementation of a framework of IS controls within an enterprise as relevant & encompassing all key areas. The primary objective of GEIT are to analyse and articulate the requirement for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, and practices, with the clarity of responsibilities and authority to achieve the enterprise missions, goals and objectives.

Benefits

- It provides **consistent approach** integrated and aligned with the enterprise governance approach.
- It ensures that IT-related **decisions** are made **in line with** the enterprise's strategies and objectives.
- It ensures that IT **related processes** are **overseen** effectively and transparently.
- It confirms **compliance** with legal and regulatory requirement.
- It ensures that the **governance requirements** for board members are **met**.

Key management Practice of IT Compliance

Briefly describes the Key management Practice provided by COBIT 5 for ensuring IT Compliances**. (Nov, 15)**

- ✓ **Identify External Compliance requirement:**
- ✓ **Optimise Response to external Requirements:**
- ✓ **Confirm External Compliance:**
- ✓ **Obtain assurance of External Compliance:**

COBIT 5:

Discuss the COBIT 5 & its components in brief? **(RTP-15M)**

Discuss key benefits of COBIT5 Framework **(RTP)**

These are as follows

- A comprehensive framework such as COBIT 5 enables enterprise in achieving their objectives for the governance and management of enterprise IT.
- The best practice of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk level and resources use.
- Further, COBIT 5 enables to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.
- COBIT 5 helps enterprises to manage IT related risk and ensure compliance, continuity, security and privacy.
- COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.
- The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
- COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

What do you understand by the terms COBIT 5? Describe its practices in brief. **(MT 14N)**

What is COBIT 5? Why there is a need of enterprise to use COBIT 5 (MT 15M)

It helps enterprise to create optimal value from their information and technology. यह provide करता है the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decision through simplified navigation and use.

COBIT is a set of best practices or framework for IT management created by **Information Systems Audit & Control Association (ISACA)** & **IT Governance Institute (ITGI)** in **1996.**

COBIT provides a set of generally accepted indicators, processes & best practices to assist them in maximizing benefits derived through use of IT.

Five Principles of COBIT 5 (MCA SE) **(May 15)**

The 5 key principles for governance and management of enterprise taken together enable the enterprise to build an effective governance and management framework that optimise technology investment and use.

- **M. Meeting Stakeholder Needs:**
- **C:-Covering Enterprise End to End**
- **A:-Applying Single Integrated Framework**
- **E:-Enabling a Holistic Approach**
- **S:-Separating Governance From Management**

© **Principle 1: Meeting Stakeholder Needs -** COBIT 5 provides all of the **required processes and other enablers** to support business value creation through the use of IT. 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 and practices.

© **Principle 2: Covering the Enterprise End-to-End -** COBIT 5 **integrates** governance of enterprise IT **into enterprise**

governance. COBIT 5 **covers** all functions and processes within the enterprise **and considers** all IT related governance and management enablers **to be enterprise-wide and end-to-end.**

- © **Principle 3: Applying a Single Integrated Framework -** COBIT 5 is a single and integrated framework **as it aligns with** other latest relevant standards and frameworks, thus **allowing the enterprise to use** COBIT 5 as the overarching governance and management framework integrator.
- © **Principle 4: Enabling a Holistic Approach -** COBIT 5 defines **a set of enablers** to support the implementation of a **comprehensive** governance and management system for enterprise IT that require a holistic approach, taking into account several interacting components.
- © **Principle 5: Separating Governance from Management -** The COBIT 5 framework **makes a clear distinction** between governance and management. These two disciplines **encompass different types** of activities, require different organizational structures and serve different purposes.

Governance: It ensures that stakeholder **needs**, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most of the enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

Management: It plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most of the enterprises, management is the responsibility of the executive management under the leadership of the Chief Executive Officer (CEO).

Seven Enablers of COBIT 5: (POPSIP)

Discuss the 7 enabler of COBIT 5 **(MT 14N)**

Write short notes on COBIT 5 Enablers **(May, 14)**

COBIT 5 framework describes seven categories of enablers, which are given as follows:

- **Principles, policies and frameworks** are the **vehicle to translate** the desired behaviour into practical guidance **for day-to-day management.**
- **Processes** describe **an organized set** of practices and activities **to achieve certain objectives** and **produce a set of outputs** in support of achieving overall IT-related goals.
- **Organizational structures** are the key **decision-making entities** in an enterprise.
- **Culture, ethics and behaviour** of individuals and of the enterprise are **very often underestimated** as a success factor in governance and management activities.
- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is **required** for keeping the organization **running and well governed**, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, infrastructure and applications** include the infrastructure, technology and applications that **provide** the enterprise **with information technology processing and services.**
- **People, skills and competencies** are linked to people and are **required** for successful completion of all activities and for making correct decisions and taking corrective actions.

Governance: It ensures (make sure) that stakeholder needs (आवश्यकताऐं), conditions (परिस्थितियाँ) and options (विकल्पें) are evaluated (मुल्यांकन) to determine (तय करना के लिए) balanced, agreed-on objectives to be achieved; setting direction through prioritization and decision making के द्वारा; and **monitoring (**keep an eye on) performance and compliance **against** agreed-on direction and objectives**.**

Management: It plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

Write short note on Internal Controls as per COSO **(Nov, 14)**

As per COSO, Internal Control is comprised of five interrelated components:

→ **Control Environment:** For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.

→ **Risk Assessment:** Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

→ **Control Activities:** Control activities must be developed to manage, mitigate, and reduce the risks associated with each

business process. It is unrealistic to expect to eliminate risks completely.

→ **Information and Communication:** Associated with control activities are information and communication systems. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

→ **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions

The key management practices, which are required for aligning (arrange in a line) IT strategy with enterprise strategy;

Discuss key management practices required for aligning IT Strategy with Enterprise Strategy. **(May 15) (RTP-15M)**

-:UA DC DC:-

- **Understand Enterprise Direction (दिशा):** This **considers** the current enterprise environment and business processes; enterprise strategy and future objectives and also the external environment of the enterprise.
- **Assess the current environment, capabilities and performance:** This **assesses** the performance of current internal business and IT capabilities and external IT services, and **develops** an understanding of the enterprise architecture in relation to IT.
- **Define the target IT Capabilities**: This defines the target business and IT capabilities and required IT services **on the basis of enterprise environment and requirements**; assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices.
- **Conduct a Gap Analysis:** This **identifies** the gaps between the current and target environments and **considers** the alignment of assets with business outcomes to optimize investment.
- **Define the strategic plan and road map:** This creates a strategic plan **that defines**, in cooperation with relevant stakeholders, **how IT- related goals will contribute** to the enterprise's strategic goals.
- **Communicate the IT strategy and direction**: This creates **awareness and understanding** of the business and IT objectives and direction, **as captured in the IT strategy**.

The key management practices for evaluating risk Management are given as follow (EVM)

(a)Evaluate Risk Management

(b)Direct Risk Management

(c)Monitor Risk Management

(a)Evaluate Risk Management: This continually examines & makes judgement on the effect of risk on the current & future use of IT in the Enterprise. This further considers whether the enterprise's risk appetite is appropriate & that the risk to the enterprise value related to the use of IT are identified and managed.

(b)Direct Risk Management: This direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite**.**

(c)Monitor Risk Management: This monitors the key goals & metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation. **(RTP-15M)**

GEIT & benefit (**RTP 14N**)

Discuss the key Management Practices for implementing risk management (**RTP 14N) (MT Nov, 14)**

The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective**.(May, 15)** (6 Marks)

Key Management Practices for this purpose are given as follow

(a)Collect data: To enable effective IT related risk identification, analysis and reporting.

(b) Analyse the Risk: Develop useful information to support risk decisions.

(c) Maintain a risk profile: Maintain an inventory of known risks and risk attributes.

(d) Articulate Risk: To inform IT- related exposures and opportunities to all required stakeholders for appropriate response. **(e) Define a risk management action portfolio**: To manage opportunities and reduce risk to an acceptable level as a portfolio.

(f) Respond to the risk: To respond limit the magnitude of loss from IT related events in a timely manner.

Evaluating IT Governance Structure and Practices by Internal Auditor

It outlines/explain specific areas and critical aspects relating to Governance Structure and Practices, which can be reviewed as part of Internal Audit. Internal audit evaluate several key components that **leads to effective** governance. These are explained here;

- Leadership
- Organisational structure
- Processes

- Risks
- Controls
- Performance Monitoring/Measurement

Sample areas of GRC for review by Internal Auditors(RTP 14N)

→ **Scope**: Evaluate & Contribute to the improvement of GRC process using systematic & disciplined approach.

→ **Governance:** Assess & make appropriate recommendation for improving G process in its accomplishment of following objective:

→ **Evaluate Enterprise Ethic:** Evaluate the design & implementation & effectiveness of the organisation ethics related objectives, programs and activities.

→ **Risk Management:** Evaluate the effectiveness & contribute to the improvement of RMP.

→ Interpretation:

→ **Risk Management Process**: Gather information to support this assessment during multiple engagements. The result of these engagements provide an understanding of the organisation's RMP and its effectiveness.RMP monitored through on-going management activities, separate evaluations, or both.

→ **Evaluate Risk Exposures:** Evaluate risks exposures relating to the organisation's G, O, & IS regarding the:

→ **Evaluate Fraud and Fraud Risk:** Evaluate the potential for occurrence of fraud & how the organisation manages fraud risk.

→ **Address Adequacy of Risk Management:** Address risk consistent with the engagement's objectives & be alert to the existence of other significant risks. Incorporate knowledge of risks gained from consulting engagement into auditor evaluation of the organisation RMP. Refrain from assuming any management responsibility by actually managing risks.

Sample Areas of Review of Assessing and Managing Risks

Evaluating and Assessing the System of Internal Controls

The key management practices for Evaluating and Assessing the System of Internal Controls in an enterprise are given as follows: (**RTP 14N**)

You are appointed by a leading enterprise to assess and to evaluate its system of IT internal controls. What are the key management practices to be followed to carry out the assignment complying with COBIT 5? **(Nov, 14)**

- **Monitor Internal Controls**: Continuously, benchmark and improve the C environment & C framework to meet the organisational objective.
- **Review Business Process Controls Effectiveness**: Review operation of controls, monitoring and test evidence **to ensure** that controls within the business processes **operate effectively**. Maintain evidence of the effectiveness of control through the mechanism such as periodic testing of controls, continuous control monitoring, independent assessments, command & control centre, and network operation centres. This **provides business with the assurance** of control effectiveness to meet requirement related to business, **regulatory & social responsibilities**.
- **Perform Control Self-assessment**: Encourage management & process owner **to take positive ownership** of control improvement through a continuing program of self-assessment **to evaluate completeness and effectiveness** of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiency**: ICF & analyse & identify **their underlying root causes**. Escalate control deficiency & report to stakeholders.
- **Ensure That assurance providers are independent and qualified**: Independent from the function, groups or organisations in scope. Demonstrate appropriate attitude & appearance, competence in skill & knowledge **necessary to perform assurance**, & **adherence to code** of ethics and professional standards.
- **Plan assurance initiatives**: Based on enterprise objective & conformance objective, assurance objectives & strategic priorities, inherent risk, resource constraints & sufficient knowledge of the enterprise.
- **Scope assurance initiatives**: Define & agree with management on the scope of the assurance initiatives, based on assurance objectives.
- **Execute assurance initiatives**: Execute planned assurance initiatives. Report on identified finding. Provide positive assurance opinions, where appropriate, & recommendation for improvement relating to identified operational performance, external compliance & internal controls residual risk.

Discuss different levels of managerial activity that are carried out in an enterprise. RTP

There are three levels of managerial activity in an enterprise which are as follows:

→ **Strategic Level:** it is defined as the process of deciding on objective of the enterprise, on changes in these objectives, on the resources used to attain these objectives and on the policies that are to govern the acquisition, use and disposition of these resources. Strategic planning is the process by which top management determines overall organisational purpose and objectives and how they are to be achieved. Corporate-level strategic planning is the process of determining the overall character and purpose of the organisation, the business it will enter and leave, and how resources will be distributed among those businesses.

→ **Management Control:** It is defined as the process by which manager assures that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.

→ **Operational Control:** It is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

Chapter 2: Information System Concept

Information

What is information? Discuss different attributes of information. **(RTP-15M)**
Discuss different attributes of useful and effective information. **(MT –Nov, 14)**
Define the term "Information". Discuss various important attributes that are required for useful and effective information**. (Nov, 11)** What do you mean by Information? Describe the important characteristics of information, which makes it useful to the organization. **(MAY 2006)**

Technically, information means processed data **that have been put into a meaningful and useful context**. Data consists of facts, values or results, and information is **the result of relation between data** e.g. in a spread sheet student name, roll number and marks obtained in science and arts subjects represents data whereas the graph that shows the percentage of students, who acquired more than 80% in science subjects and 65% in arts subjects represents information. Information May be represented in the form of text, graph, pictures, voice, videos etc.

Mere collection of data is not information and mere collection of information is not knowledge. Information relates to description, definition, or perspective (what, who, when, where). Information is essential because it adds knowledge, helps in decision making, analyzing the future and taking action in time. Information products produced by an information system can be represented by number of ways e.g. paper reports, visual displays, multimedia documents, electronic messages, graphics images, and audio responses.

Attributes of information Some of the important attributes of useful and effective information are given as follows: (M FARUQ PVR Cinema)

- **M: Mode and format**: The mode of communicating the information to human should be in such a way that it can be easily understands by the people. Mode may be in the form of voice and text, combination. Format should be designed in such way that it assist in decision making. Diagram, graphs, curves are suited for presenting statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.
- **F: Frequency:** For example- weekly reports of sales show little change as compared to the quarterly reports and contribute less for assessing salesman capability.
- **A: Availability**: Information is useless if not available at the time of need.
- **R: Rate**: The rate of transmission of information can be represented by the time required to understand a particular situation. Useful information is one which is transmitted at a rate which matches with the rate at which recipient wants to receive.
- **U: Updated/Current:** The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed intervals of time so that the current score will be available. Similar is the case with broker who wants the latest information about the stock market.
- **Q: Quality:** Correctness of information. For example, the correct status of inventory is highly required.
- **P: Purpose:** Information must have purpose at the time it is transmitted to a person, otherwise it is simple data. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises
- **V: Validity:** It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee does not support evaluating his performance.
- **R: Reliability: –** It is a measure of failure or success of using information for decision-making. If information leads to correct decision on many occasions, we say the information is reliable.
- **C: Completeness and adequacy:** The information provided should be complete and adequate in itself because only complete information can be used in policy making.
- **T: Transparency:** It is essential in decision and policy making. For example, giving only total amount of advances does not give true picture of utilization of funds for decision about future course of action; rather deposit-advance ratio May be more transparent information as it gives information relevant for decision making.
- **V: Value of information:** It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision-maker May select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information.

System: A system is a group of **inter connected** components working towards accomplishment of a common goal by

accepting input and producing output **in ordered** transformation process. (जब दो या दो से अधिक components मिल जाते हैं और एक साथ ordered fashion मे काम करते है किसी predefined objective को achieve करने के लिए then this is called system)

यंत्र: दुनीया का कोई भी **यंत्र पूर्वनिर्धात काम को पूरा करने के लिएं बनाया जाता है** For example water pump, computer, motor cycle, truck tec.

A system generally consists of input, processing, storage and output.

Input is data entering the system

Processing is the manipulation of input data.

Output is the data given by the system after processing.

Storage refers to the storage of data for the current or future use.

Classification of System on the basis of:

- ✓ Behaviour
- ✓ Element **(RTP-15M)**
- ✓ Degree of human intervention
- ✓ Working/Output

Behaviour based classification of system:

Differentiate between open and closed systems. **(MAY, 07)**

Write short notes on Closed and open systems **(May, 08)**

Open System: It interacts with other systems in its environment. Interaction is by way of taking input from and returning output to the environment. It also changes itself with the changes in its environment. Information System is an example of open system.

Closed System: It does not interact with environment and does not change with the changes in environment.

Identify and justify the type of each one of the following systems based on how they perform within an environment and/or certainty/ uncertainty:

- ❖ Marketing system
- ❖ Communication system
- ❖ Manufacturing system
- ❖ Pricing system
- ❖ Hardware-Software system.**(Nov, 09)**

Sub-system	System Type	Justification
Marketing System	Open System	The marketing system plays a pivotal role in the running of a business in the competitive environment. The objective of the system is to maximize customer satisfaction by providing a free interactive environment. The system takes input/feedbacks and facilitates the outcomes as products of the company and to create new customers.
Communication System	Open System	The communication system in a organization is a point of contact to balance the external influence and render its services to the customers. The system interacts freely with its environment by taking input and returning output.
Manufacturing System	Closed System	This system is in place to meet a particular objective. It does not interact neither with the environment nor changes with the change in the environment. A manufacturing unit is completely isolated from its environment for its operation.
Pricing System	Probabilistic and Open System	The system has a probable behavior and interacts freely with its environment by taking inputs and returning outputs. The pricing system is a dynamic one which influences the form of profiand goodwill of an organization.
Hardware-Software System	Closed Deterministic System	Since the interaction among the parts of the system is known with certainty and does not interact with the environment and does not change with the change in the environment. Here the requirements of the hardware and software inventory are known with certainty. The operational state of these systems is in predictable manner.

Information System:

Q. Discuss IS and its components. What are the activities carried out by IS in general? (**MT, 15M**)

It comprises people, hardware, software, data and network.

Enumerate the characteristics of a Computer Based Information System. **(May, 11)**

Characteristics of Computer Based Information system are:

- ✓ All Systems **works for predetermined objectives** (पुर्वनिर्धति ऊद्देश्य or well defined) and the system is **designed and developed accordingly.**
- ✓ In general a system has **number of interrelated and interdependent subsystems or components**. No subsystem cam function in isolation; it depends on other subsystem for its input. (एक system के बहुत सारे भाग होते हैं और ए सभी एक दुसरे पर निभर होते हैं)
- ✓ If one subsystem or component of a system fails; in most cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.(अगर एक भाग fail हो जाता हैं तब पुरी system fail हो जाता है)
- ✓ The way a subsystem work with other subsystem is called **interaction**. The different subsystems interact with each other **to achieve the goal of the system.** (भागों का आपसी लेनदेन को interaction कहते हैं और वै ऐसा इसलिए करते है ताकी system का predetermined objective पुरा हो सके)
- ✓ The work done by individual subsystem is **integrated to achieve the central goal of the system.** The goal of individual subsystem is of **lower priority** than the goal of the entire system.

Discuss major areas of Computer- Based applications. (RTP)
Major areas of computer based applications are (i) Finance & accounting, (ii)Marketing & sales, (iii) Inventory/store management, (iv)HRM.

Types of Information System

System analysts develop various categories of information systems to meet a variety of business needs. Discuss any three such systems briefly. (**NOV, 07) Briefly state following**

Operations Level Systems: Here Systems are required **to process** the data **generated** and **used** in business operation.

→ Transaction Processing Systems.

Management Level System: Here Systems **support** manager in effective decision making **by providing relevant and required information** at the right time to right people.

- ✓ **Management Information Systems,** and
- ✓ **Decision Support Systems.**

Strategic level Systems: Here systems **support** the senior level management **to tackle and address** strategic issues and long term trends, both inside organisation and the outside world.

- Executive Information Systems

Knowledge Level Systems: Here systems support **discovery, processing and storage** of knowledge and data of worker.

- ❖ Office Automation Systems:
  - ➢ **Tex Processing Systems,**
  - ➢ **Electronic Document Management Systems,**
  - ➢ **Electronic Message Communication Systems,** and
  - ➢ **Teleconferencing and Video conferencing Systems.**
- ❖ Knowledge Management System:

Specialized Systems: These systems **also support** either operations or management applications.

- **Expert Systems,**
- **Cross Functional Information Systems,** and
- **Core Banking System.**

Operation Level System:

Transaction Processing Systems: (**RTP 14N**)

Define Transaction Processing System (TPS). List out the salient features of a TPS. **(Nov, 13)**

These systems are aimed at **expediting and improving** the routine business activities that **all organizations engage**. **Standard** operating procedures, which **facilitate handling of transactions**, are often **embedded in computer programs** that control the entry of data, processing of details, search and presentation of data and information. TPSs if properly computerized provide **speed and accuracy** and can be programmed **to follow** routines **without any variance**.
It is an IS that manipulate data from business transactions.

Manipulation: It means organising business transactions in files or database.
Business Transactions: Sales, Purchases, Receipts, payments, Delivery, Production.
Business Transaction is manipulated to provide information required by different operation (यह कहना अच्छा होगा की it provide information to respective departmental manager such as sales manager regarding sale volume achieved, production manager regarding production volume.)
Typically, a TPS involves the following activities;

- → **Capturing data to organise in files or database;**
- → **Processing files/database using application software;**
- → **Generating information in the form of report; and**
- → **Processing of the queries from the various quarters of the organisation.**

Components of TPS

- **Input**: Source documents are the physical evince of inputs into the TPS.
- **Processing**: Use of journal and ledger to provide a permanent and chronological record.
- **Storage**: Ledger and files provide storage of data on both manual and computerised systems.
- **Output**: Any document generated from the system is output.

What are the basic features of TPS? **(MT- Nov, 14)**

Features of TPS (LAB SIOS)

- **Large Volume of Data:** As TPS is transaction – oriented, it generally consists **large volumes of data** and thus **requires greater storage capacity.** Their **major concern** is to ensure that the data regarding the economic events in the organizations are **captured quickly and correctly.**
- **Automation of Basic Operation:** Any TPS **aims at automating** the basic operations of a business enterprise and plays **a critical role** in day-to-day functioning of the enterprise. **Any failure** in the TPS for a short period of time can **play havoc** with the functioning of the enterprise. Thus, TPS is an **important source** of up-to-date information regarding the operations in the enterprise.
- **Benefits are easily measurable:** TPS **reduces** the workload of the people associated with the operations and **improves** their efficiency **by automating some of the operations**. Most of these benefits of the TPS are tangible and easily measurable. Therefore, cost benefit analysis regarding the desirability of TPS is easy to conduct. As the benefits from TPS are mainly tangible, the user acceptance is easy to obtain.
- **Source of input for other systems:** TPS is the **basic source of internal information** for other information systems. Heavy reliance by other information systems on TPS for this purpose makes TPS important for tactical and strategic decisions as well.

An owner of a small local store is currently using manual system for his day to day business activities viz. purchase, sales, billing, payments receipts etc. In the last few years, turnover of the store is increased manifold and now it has become increasingly difficult to handle all these activities manually. You being an IT expert and his auditor, are requested to suggest **which operation support system will be most suitable for him**. Also advise him what activities can be performed by the proposed system and what are major limitation of it. **(May, 14)**

In the given scenario, **we would suggest** the owner of the local store to go for Transaction Processing System (TPS), which will be the **most suitable option** for him. **Because** TPS at the lowest level of management is an information system that manipulates data from business transactions efficiently and if properly computerized, TPS provides speed and accuracy too. Various day-to-day business activities such as sales, purchase, production, billing, payments or receipts involves transactions and these transactions are **to be organized and manipulated** to generate various information products for external use.

Following are the major activities, which can be performed by the proposed TPS:

- Capturing data to organize in files or databases;
- Processing of files / databases using application software;
- Generating information in the form of reports;
- Processing of queries from various quarters of the organization.

A TPS May **follow periodic data preparation** and batch processing (as in payroll application) or on-line processing (as in inventory control application). In industries and business houses, **now-a-days**, **on-line approach is preferred** as it provides information with up-to-date status. However, the people involved in TPS, usually are not in a position to take any management decision. This is the major limitation of it.

Management level Systems

Management Information System (MIS)

An integrated user-machine system designed for providing information to support operational controls, management controls and decision making functions. MIS decision maker को information provide करता है क्योंकि problem routine nature का है, information required for making decision मालुम है.

Explanation

यहाँ हमे क्या information चाहिए होता है control and decision making के लिऐ वह हमे advance मे हि मालुम होता है, इसलिए तो हम MIS develop कर पाते है. Because pre-requisite for developing any system is that the system will be designed and developed for predetermined objective. दुनीया का कोई भी **यंत्र पूर्वनिर्धात काम को पूरा करने के लिऐं बनाया जाता है**

MIS has been defined by Davis and Olson as "An integrated user-machine system designed **for providing information** to support operational control, management control and decision making functions in an organization". Another notable definition of MIS is **"***MIS is a computer based system that* **provides flexible and speedy access** *to accurate data".*

MIS support managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill organizational goals. Nature of MIS at different levels has different flavors and they are available in the form of reports, tables, graphs and charts or in presentation format using some tools. MIS at the top level is much **more comprehensive** but is condensed or summarized compared to the information provided to those at middle level management. MIS can help in making effective, structured reports relevant for decisions of day-to-day operations. These reports and displays can be made available on demand, periodically or whenever exceptional conditions occur.

Characteristics of MIS (ODIC HSCC)

Describe any six characteristics of an effective management information system. **(Nov, 13)**

"MIS support manager at different level to take decision to fulfill the organisation goals." Explain the major characterise of MIS to achieve these goals. **(Nov, 15)**

State the factors to be considered for designing an effective Management Information System. **(NOV, 06)**

- Management **o**riented: Development of IS start from **an appraisal management needs and overall business objectives**.
- Management **D**irected: Direct the system development effort. Devote sufficient time.
- Integrated: An integrated system has the capability **to generate more meaningful information** to management as it takes a comprehensive view at the interlocking sub-systems that operated within a company.
- **C**ommon Data Flows: Use of common input, processing and output procedures and media whenever required. This **eliminates duplication** in data collection, **simplifies** operation and produces an **efficient** IS.
- **H**eavy Planning Element: MIS developer **must be present** in MIS development and should **consider future enterprise objectives and requirements** of information **as per the organisation structure** of the enterprise **as per requirement**.
- **S**ub System Concept: IS must be **broken down into** digestible sub-systems, which can be implemented one at a time by developing phasing plan. This breaking down sets the stage for this phasing plan.
- **C**ommon Database: DB is the mortar that **holds functional systems together**. DB can be **accessed by several information sub-systems** and **eliminate the necessity of duplication** in data storage, updating, deletion and protection.
- **C**omputerised

Misconception about the MIS (RTP 14N)

- ✓ Any CBIS is MIS
- ✓ Any reporting System is MIS
- ✓ A Management technique
- ✓ A bunch technologies
- ✓ An implementation of organisational systems and procedures.
- ✓ The study of MIS is about use of computers.
- ✓ More data in generated report more information to managers.
- ✓ Accuracy plays vital role in reporting.

Pre-requisites of an effective MIS

Describe the major pre-requisites of a Management Information System to make it an effective tool. **(May, 14)**

Describe the main pre-requisites of a Management Information System, which makes it an effective tool. (**MAY, 05)**

- **Database,**
- **Qualified System and management staff,**
- **Support of top management, and**
- **Controls and maintenance of MIS.**

The main pre-requisites of an effective MIS are as follows:

(A)Database: It can be defined as a "superfile" which **consolidates data** records **formerly stored** in many data files. The data in a database is **organized** in such a way that **access to the data** is **improved and redundancy** is **reduced**. **The characteristics** of database are:

→ The database is **sub-divided** into major information subsets needed to run a business wherein each subsystem **utilizes same data and information** kept in same file to satisfy its information needs.
→ It is user-oriented.
→ It is capable of being used as **a common data source**, to various users, helps in avoiding duplication of efforts in storage and retrieval of data and information.
→ It is available to **authorized persons only**.
→ It is **controlled** by a separate authority established for the purpose, known as Data Base Management System (DBMS).
→ The **maintenance** of data in database **requires** computer hardware, software and experienced computer professionals.

(B)Qualified system and management staff: The second pre-requisite is that it should be **manned by qualified officers**. For this, the organisational management base should comprise of two categories of officers.

→ **Systems and Computer experts**: They, in addition to their **expertise** in their subject area should **be capable of understanding management concepts** to facilitate the understanding of problems faced by the concern. They should **also be clear** about the **process of decision making and information requirements** for planning and control functions.
→ Management experts: They should understand quite **clearly the concepts and operations** of a computer.

(C)Support of Top Management: The MIS **to be effective**, should **receive the full support** of the top management. The **reasons** for this are as follows:

→ Subordinate managers are **usually lethargic** about activities which do **not receive the support** of their superiors.
→ The **resources** involved in computer-based information systems are **large** and are growing larger in view of importance gained by management information system.
→ Their whole hearted **support and cooperation** will help in making MIS **an effective one**.

(D) Control and Maintenance of MIS: Control of the MIS means the **operation of the system** as it was **designed to operate**. Sometimes users **develop their own procedures** or short cut methods to use the system, **which reduce its effectiveness**. To check such habits of users, the management at each level in the organization should **device checks for the information system control**. At times, there May be the need **for improvements to the system**. Formal method and documenting always must be provided. Maintenance is closely related to control.

(E)Evaluation of MIS:

An effective MIS should be **capable of meeting** the information requirements of its executives **in future as well**. The capability **can be maintained** by evaluating the MIS and taking **appropriate timely action**. The evaluation of MIS should take into account the following points:

- Examining the **flexibility** to cope with future requirements ;
- Ascertaining the **view of the users and designers** about the capabilities and deficiencies of the system ;
- Guiding the appropriate authority about the **steps to be taken to maintain effectiveness** of MIS.

Constraint in implementing a MIS: (**RTP 14N**)

Discuss the constraints in operating a MIS. **(May, 12)**

Discuss the limitations of the Management Information system. **(MAY 2006)**

→ Non-availability of expert, who can **diagnose the objective of the organisation** and provide desired direction for installing a system, which operates properly.
→ Expert usually **faces the problem** of selecting which sub-system of MIS should be installed and operated first.
→ Due to **varied objectives** of the business concerns, the approach adopted by experts for designing and implementing MIS is **non-standardised.**
→ **Non-cooperation** from staff is **crucial problem**, which should be handled tactfully.

Limitation of MIS: (**MT 15M**)

Write short notes on Limitations of MIS **(Nov, 12)**

♦ The **quality** of the output of MIS is basically governed by the **quality of input & Process**.
 It is **not substitute** for effective management. It is merely an **important tools** in the hands of executives **for decision making and problem solving.**

- It may not have **requisite flexibility to quickly update itself** with the changing needs of time**, especially in fast changing and complex environment.**
- It cannot provide **tailor made information package** suitable for every type of decision made by the executive.
- It takes into account **only quantitative factors**, ignores the **non-quantitative factor**.
- It is less useful for **non-programmed decision**.
- Its effectiveness is reduced, where **culture of hording** and not sharing information prevail;
- Its effectiveness deceases due to **frequent change in top management**.

Discuss the potential impact of computers and MIS at the top level of Management. (**Nov, 2003)**

The potential impact of computers on top-level management May be **quite significant**. An important factor, which May account for this change, is the **fast development** in the area of computer science. It is believed that in future computers would be able to provide **simulation models** to assist top management in planning their activities. By using **sensitivity analysis** with the support of computers, it May be possible **to study and measure the effect of variation** of individual factors **to determine final results.** Also, the availability of a new class of experts will **facilitate effective communication with computers**. Such experts May also play **a useful role in the development and processing of models.** In brief, potential impact of computers would be more in the area of planning and decision-making.

Futurists believe that in future, top management will **realize the significance of** techniques like simulation, sensitivity analysis and management science. The **application** of these techniques **to business problems** with the help of computers would **generate accurate, reliable, timely and comprehensive information to top management**. Such information will be **quite useful for** the purpose of managerial planning and decision-making. Computerized MIS will **also influence** in the development, evaluation and implementation **of a solution to a problem** under decision-making process.

Decision Support System (DSS)

"A decision support system supports the human decision-making process rather than providing a means to replace it". Justify the above statement by stating the characteristics of decision support system. (**MAY 2005)**

What is Decision Support System? Discuss its characteristics in brief. **(May, 12)**

It is a type of Compr infrom system that supports business and organisational decision making activities.

DSS केवल साहायता करता है decision maker को, information नहीं provide करता है, क्योंकि problem requiring decision unique है, और information requirement keeps on changing क्योंकि situation surrounding problem भी change होते रहता है । In such case a system with pre-determined objective cannot be designed and developed.

DSS is intended to help decision maker to compile (संगृहीत करने मे) useful information from raw data, documents, personal knowledge, and/or business model to identify and solve problem and make decision. एक system जो tool provide करता है the manager को, manager के मदद के लिए in solving semi-structured and unstructured problem in manager own way.

A decision support system (DSS) is defined as a system **that provides tools** to managers to assist them in solving **semi-structured and unstructured** problems in their own way. A DSS is **not intended** to make decisions for managers, but rather **to provide managers with a set of capabilities** that enables them **to generate** the information required by them in making decisions.

Characteristics of DSS: Discuss the characteristic of DSS **(MT 14N)**

- ✓ This support decision making and occur at all level of management.
- ✓ Instead of helping individuals working on independent tasks, it should be able to help group making decisions.
- ✓ It should be flexible and adaptable.
- ✓ It focuses on decision rather on data and information.
- ✓ It can be used for structured problems.
- ✓ User friendly.
- ✓ Extensible and evolve over time.
- ✓ Mainly used for decision making rather than communicating decision and training purpose.
- ✓ Easy to use.

Components of DSS: Briefly discuss four basic components of Decision Support System. **(May, 08)**

1. **The user**
   a. **Manager**
   b. **Staff specialist**
2. **Database**
3. **Planning language**
   a. **General Purpose**

b. Special Purpose

4. **Model Base**:

A decision support system has the following components:

(i) **The User:** The user of a DSS is usually a manager **with an unstructured or semi-structured problem** to solve. Users do **not need a computer background** to use a DSS for problem solving. The most **important knowledge** is a thorough understanding of the problem and the factors to be considered in finding a solution. A user does **not need extensive education** in computer programming in part **because** a special planning language **performs the communication** function within the DSS.

(ii) **One or more databases:** DSS **include** one or more databases which **contain both** routine and non-routine data from both internal and external sources. The data from external sources **include** data about the operating environment surrounding an organization. DSS users **May construct additional database** themselves. Some of the data May come from internal source.

(iii) **A planning language:** Two types of planning languages that are commonly used in DSS are (1) general purpose planning languages and (2) special purpose planning languages. General purpose planning languages allow users **to perform many routine tasks** like-retrieving various data from a database or performing statistical analysis. The languages in most electronic spreadsheets are good example of general purpose planning languages. These languages enable the user to tackle a broad range of budgeting, forecasting and other worksheet oriented problems. Special purpose planning languages are **more limited**. Some statistical languages, such as SAS, SPSS and Minitab are examples of special purpose planning languages.

(iv) **Model Base:** The model base is the "brain" of the DSS because it **performs data manipulation and computations** with the data provided to it by the user and the database. **There are many types of model bases but most of them are custom-developed models that do some type of mathematical functions**. The analysis provided by the routine in the model base is the key to supporting the user's decision.

Example of DSS in Accounting:

DSSs are widely used as part of an organisation's Accounting Information System. Give example to support this statement. **(May, 07)** **OR** Discuss various examples of DSS in Accounting.

DSSs are widely **used as a part of an organization's Accounting Information System**. The complexity and nature of DSSs vary. Many are **developed in-house** using either a general type of **decision support program or a spreadsheet program** to solve specific problems. Below are several illustrations:

- ✓ **Cost Accounting System:** The **health care industry** is well known for its **cost complexity**. Managing costs in this industry **requires controlling costs** of supplies, expensive machinery, technology, and a variety of personnel. **Cost accounting applications** help health care organizations **calculate product costs** for individual procedures or services. DSSs can **accumulate these product costs** to calculate total costs per patient. Health care managers many **combine** cost accounting DSSs **with other** applications, such as productivity systems. Combining these applications **allows** managers **to measure the effectiveness** of specific operating processes. One health care organization, for example, **combines** a variety of DSS applications **in productivity**, **cost accounting, case mix, and nursing staff scheduling** to improve its management decision making.
- ✓ **Capital Budgeting System:** Companies **require** new tools **to evaluate high-technology investment** decisions. Decision makers need **to supplement** analytical techniques, such as net present value and internal rate of return, **with** decision support tools **that consider some benefits of new technology not captured in strict financial analysis**. **One** DSS **designed** to support decisions about investments in automated manufacturing technology **is Auto Man**, which **allows** decision makers **to consider** financial, nonfinancial, quantitative, and qualitative factors **in their decision-making processes**. Using this DSS, accountants, managers, and engineers **identify** and
- ✓ **Budget Variance Analysis:** Financial institutions **rely heavily** on their budgeting systems **for controlling costs and evaluating managerial performance.** One institution **uses a computerized** DSS **to generate monthly** variance reports for division comptrollers. The system **allows** these comptrollers **to graph, view, analyze, and annotate** budget variances, as well as **create additional** one-and five-year budget projections **using the forecasting tools** provided in the system. The DSS thus **helps** the comptrollers **create and control budgets** for the cost-center managers reporting to them.
- ✓ **General DSS:** As mentioned earlier, some planning languages used in DSSs are general purpose and **therefore have the ability to analyze many different types of problems**. In a sense, these types of DSSs are a decision-maker's tools. The **user needs** to input data and answer questions about a specific problem domain **to make use of this type** of DSS. An example is **a program called Expert Choice.** This program **supports** a variety of problems **requiring** decisions. The **user works interactively with** the computer **to develop** a hierarchical model of the decision problem. The DSS **then asks the user** to

compare decision variables with each other. For instance, the system might ask the user how important cash inflows are versus initial investment amount to a capital budgeting decision. The decision maker also makes judgments about which investment is best with respect to these cash flows and which requires the smallest initial investment. Expert Choice analyzes these judgments and presents the decision maker with the best alternative.

Executive Information System (RTP 14N)

What is meant by EIS? What are its characteristics? **(Nov, 12)**
What is an Executive Information system? Discuss its various purposes. **(Nov, 05)**
Write short notes on Executive Information Systems **(Nov, 03)**

It is a tool that is designed to meet the special needs of top-level managers. It provides **direct on-line access to relevant information in a useful and navigable format**. Relevant information is timely, accurate, and actionable about aspects of a business that are of particular interest to the senior manager. The useful and navigable format of the system means that **it is specifically designed to be used by individuals with limited time, limited keyboarding skills, and little direct experience with computers.** An EIS is easy to navigate so that managers can **identify broad strategic issues**, and then **explore the information to find the root causes of those issues**. EIS require large amounts of capacity and processing power within both the system and the network. Although most computer systems may contain some of the above characteristics, they can be differentiated from EIS in a number of ways. Most MIS and operational systems are based on transaction processing carried out by a variety of on-line and batched inputs. Unlike the EIS, information is usually presented **in numerical or textual form** and reporting is by exception, usually in printed report format. Also, EISs tend to be **externally-focused**, strategically-based systems using both internal **and** external data, whereas other computer systems mainly concentrate on internal control aspects of the organization.

Purposes of EIS:

(i) The primary purpose of an EIS is **to support managerial learning about an organization**, its work processes and its interaction with the external environment. Informed managers can **ask better questions and make better decisions.**

(ii) Second purpose for an EIS is to **allow timely access to information**. All of the information **contained in an EIS** can typically be obtained by a manager **through traditional methods**. However, **the resources and time required** to manually compile information in a wide variety of formats and in response to ever changing requirements **often inhibit managers from obtaining this information. Often, by the time a useful report can be compiled, the strategic issues facing the manager change, and the report cannot be used**. Timely access **also influences learning**. When a manger obtains the answer to a question, that answer typically sparks other related questions in the manger's mind. This way learning cycle continues unbroken.

(iii) Third purpose of an EIS is **commonly misperceived**. An EIS has a **powerful ability to direct management attention to specific areas** of the organization or specific business problems. Some managers look upon this as an opportunity to discipline subordinates.

(iv) Sometimes misaligned reporting systems can result in **inordinate management attention** to things that **are not so important**. An EIS system can provide information that is actually important and represents a balanced view of the organization's objectives.

It creates a generalised computing and communication environment rather than providing any preset applications or specific competence. यह एक समान्या computing and communication वातावरण स्थापित करता है but does not provide any pre-determined applications.

Characteristics of EIS: (RTP 14N)

- ✓ It is a CBIS that **serves information needs** of top executive.
- ✓ It enables user to **extract summary data and model complex**, problems **without the need** to learn query languages, statistical formula.
- ✓ It provides **rapid access** to timely information and **direct access** to management reports.
- ✓ It is **capable of accessing** both internal and external data.
- ✓ It provides **extensive online tool** like trend analysis, market condition etc.
- ✓ It can be **easily given** as a DSS support for decision making.

Five characteristics of the types of information used in executive decision making are given as below.

- ✓ Lack of structure;
- ✓ High degree of uncertainty
- ✓ Future orientation;
- ✓ Informal source
- ✓ Low level of detail.

Content of EIS:

Briefly explain the principles to guide the design of measures and indicators to be included in EIS. (**NOV, 07)**

OR

'There is a practical set of principles to guide the design of measures and indicators to be included in an EIS'. Explain those principles in brief.

Whatever is interesting to executives? A practical set of principles to guide the design of measures and indicators to be included in an EIS is presented below:

- ✓ EIS measures must be **easy to understand and collect**. Wherever possible, data should be collected naturally **as part of the process of work.** An EIS should **not add substantially to the workload** of managers or staff.
- ✓ EIS measures must be based on **a balanced view of the organization's objective**. Data in the system should r**eflect the objectives of the organization** in the areas of productivity, resource management, quality and customer service.
- ✓ Performance indicators in an EIS must **reflect everyone's contribution** in a fair and consistent manner. Indicators should be as **independent as possible from variables outside** the control of managers.
- ✓ EIS measures must **encourage management and staff to share ownership** of the organization's objectives. Performance indicators must **promote both team-work and friendly competition**. Measures will be **meaningful for all staff,** people feel that they, as individuals, can contribute to improving the performance of the organization.
- ✓ EIS information must be **available in the organization.** The objective is to provide everyone with useful information about the organization's performance. **Information that must remain confidential be part of EIS**.
- ✓ EIS measures must **evolve to meet the changing needs** of the organization.

How does Executive Information System differs from Traditional Information System? **(May, 13)**

Executive Information Systems differs from Traditional Information Systems in many ways. The following table presents the difference on various related dimensions:

Dimensions of Difference	Executive Information System	Traditional Information System
Level of management Nature of Information Access	For top or near top executives Specific issues/problems and aggregate reports	For lower staff Status reporting
Nature Of information provided	Online tools and analysis	Offline status reporting
Information Sources Drill down facility to go through details at successive levels	More external, less internal Available	Internal Not available
Information format Nature of interface	Text with graphics User-friendly	Tabular Computer-operator generated

Q. Discuss the OAS (**MT Nov, 14**)

Office Automation Systems (OAS)

What are the types of operations into which the **different office activities** can be broadly grouped under office automation systems. **(Nov, 10)**

What are the different office activities that can be performed under office automation system? (RTP)

Office **activities** can be grouped into following types of operations:

- ❖ **Document Capture:** Document needs to be preserved.
- ❖ **Document Creation**: Preparation of document and takes up major part of the secretary's time.
- ❖ **Receipt and distribution**: Distribution of documents to designated recipient.
- ❖ **Filing, search, Retrieval and Follow up**: related these activities and takes significant time.
- ❖ **Calculation**:
- ❖ **Recording utilisation of resource**: Record keeping in respect of specific resources utilized by office personnel.

Benefit of OAS

Computer Based Office Automation System (TEET)

Office Automation Systems (OAS) is the most rapidly expanding system. Describe the broad groups of OAS based on the types of its operations. **(May, 15)**.

- ❖ **Text Processing Systems**: Commonly used components of OAS. Large proportion of office communication takes **place in writing using word of natural language**. Automate the process of development of documents. Permit use of STANDARD Stored information to produce formalised document.
- ❖ **Electronic Document Management System: CBDMS** capture information stored in documents, stored for future and make them available to the user as and when required. Linked to OAS such as text processor, EMCS etc. Useful in **remote access** of documents that is **impossible with** manual DMS. It would enable the executive **to access the document** through his NOTEBOOK COMPUTER connected to any telephone line and show it to customer, his order document in office. Very useful for internal communication. With it, the location of executives become irrelevant FOR ACCESS of DOCUMENTS.
- ❖ **Electronic Message Communication Systems**. Components of EMCS

- **E-mail**: Explain any four features of Electronic Mail**. (Nov, 12)**
  Features: electronic transmission, online development & Editing, Broadcasting & Rerouting, Integration with other IS, Portability, Economical.
- **Facsimile**: E. Communication of IMAGES of documents over telephone line. CBFS automates fax communication & permit sharing of fax facilities. It uses SPECIAL SOFTWARE and FAX SERVERS to send and receive fax messages (FM) using common communication resource. Server can AUTOMATICALLY receive and reroute FM to the intended recipient after viewing it at the central computer.
- **Voice Mail:** A variation of E-mail in which message is transmitted in digitized voice. The receiver has to dial a voice mail service using specified equipment and he can hear the spoken message in the voice of sender.

❖ **Teleconferencing and video conferencing:** This OAS helps in receipt and distribution of information involving more than two persons located at two or more different places through audio or video with or without computer system.

Other Information Systems

Expert system:

What is expert system? Discuss some its business applications. **(RTP-15M)**
What do you mean by an Expert System? Briefly explain some of the properties that potential applications should possess to qualify for an expert system development. **(Nov, 14)**
What do you mean by ES? What are the need and benefit of ES? **(MT-Nov, 14)**
What is an Expert System? List the properties which an application should posses to qualify for Expert System development.**(May, 13)**
Write short notes on Expert systems. **(May, 04)**

Expert systems are designed to **replace the need for a human expert**. They are particularly **important** where expertise is **scarce and therefore expensive.** This is **not 'number-crunching' software**, but software that **expresses knowledge in terms of facts and rules**. This knowledge will be **in a specific area**, and therefore expert systems are **not general**, as are most DSSs, which can be **applied** to **most scenarios**, an expert system for oil drilling is not of much use in solving company taxation problems.

While there May have been **a progression** from TPSs, through MISs, to decision-support and EISs, expert systems have **arisen largely from academic research** into artificial intelligence. The expert system should be **able to learn**, i.e. change or add new rules. They are developed using **very different programming languages** such as PROLOG, which are **referred to as fifth generation languages**, or expert systems shells, which can make the **process quicker and easier**. It has been **suggested** that expert systems would be **of greater use** in the tactical and strategic level. This has been the case in banking, where expert systems scrutinize applications for loans, and lower level staff accepts the system's decision. This has replaced the somewhat subjective decision-making of more senior managers.

यह एक highly developed DSS है, जो utilized करता है knowledge generally possessed by an expert to share a problem. यह नकल करता है reasoning process of human expert and decision maker को provide करता एक type का सलाह जो decision maker would receive from such expert system.

A characteristic of ES is the ability to declare or explain the reasoning process that was used to make decision.

Business application:
Accounting & finance, Marketing, Manufacturing, Personnel and General Business.

Need for expert System;

- ❖ Expert labour is expensive and scare.
- ❖ Moreover no matter how bright or knowledgeable certain people are, they can often handle only a few factors at a time

(RTP-15M)

Benefit of expert system:

- ✓ Preserve the knowledge that might lost through resignation, retirement or death of an acknowledge company expert.
- ✓ It put information into active form.
- ✓ It assists novices in thinking the way experienced professional do.
- ✓ It is not subject to human falling.
- ✓ It can be effectively used **as a strategic tool** in areas of marketing products, cutting cost and improving products.

Some properties that potential applications should possesses to qualify as ES are given as below;
Availability, Complexity, Domain, Expertise, Structure.

Major properties that an application should possess to qualify for Expert System development are given as follows:

- **Availability**: One or more experts are capable of communicating 'how they go about solving the problems to which the

Expert System will be applied'.

- **Complexity**: Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.
- **Domain**: The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.
- **Expertise**: Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- **Structure**: The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

Business applications of Expert systems for Management Support systems. **(May, 11)**

Business applications of Expert Systems for Management Support Systems are given as follows:

(i) **Accounting and Finance:** It provides **tax advice and assistance**, helping with credit authorization decisions, selecting forecasting models, providing **investment advice**.

(ii) **Marketing:** It provides **establishing sales quotas**, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.

(iii) **Manufacturing:** It helps in determining **whether a process is running correctly, analyzing** quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.

(iv) **Personnel:** It is useful **in assessing applicant qualifications**, giving employees assisting at filling out forms.

(v) **General Business:** It helps **in assisting with project proposals, recommending** acquisition strategies, educating trainees, evaluating performance.

IS performs three important roles in Business firms:

(i) Support an organisation's business processes and operations
(ii) Support business decision making
(iii) Support strategic competitive advantage

Discuss different components of ERP and its benefits.

ERP is process management software that allows am organisation to use a system of integrated applications to manage the business and automate many back office function related to technology, services and human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales and marketing. ERP model consists of four components which are implemented through a methodology and are as follows:

→ **Software component**
→ **Process Flow**
→ **Customer mindset**
→ **Change Management**

To operate IS effectively and efficiently a business manager should have following knowledge about it. **(May, 15)**

→ **Foundation concept**: It includes fundamental **business, and managerial** concepts e.g. 'what are components of a system and their functions', or 'what competitive strategies are **required'**.

→ **Information Technologies:** It includes operation, development and management of hardware, software, data management, networks, and other technologies

→ **Business Applications:** It includes **major uses** of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.

→ **Development Processes:** It comprise **how end users and IS specialists** develop and execute business/IT solutions to problems.

→ **Management Challenges:** It includes **'how the function and IT resources are maintained'** and utilized to attain top performance and build the business strategies.

IT एक subsystem है IS का, Information Technology includes Hardware, software, database, network and other devices. IT refers to the technology of the production, storage and communication and management of information using computers and micro-electronics and is crucial part of IS. Most of the business uses IT to create and process data.

Discuss the different types of information systems. **(RTP-15M)**

Discuss the different information systems that serve different organisational level **(MT-Nov, 14)**

Different information systems that serve different organisational level are given as follow:

(i)Operation Level System,

(ii)Knowledge Level System,

(iii)Management Level System, &

(iv) Strategic level System.

(i)Operation Level System: These support operational managers by keeping tracks of the elementary activities and transaction of the enterprise e.g. sales, payroll, receipt etc. These are primarily needed to answer to query like how many books are in inventory, what happens to the payment of the customers? How many hours a particulars employee works in office? To get answer of these queries; the information should be accurate, current and easily available.

(ii)Knowledge Level System: These systems support the business to integrate new knowledge into the business and control the flow of paperwork. These help the organisation's knowledge & data workers.

(iii)Management Level System: These support the middle level management in monitoring, decision making and administrative activities and are helpful in answering questions like- Are things working well and in order? These provide periodic report rather than instant information on operations. For example- a colloge control system gives report on the number of leaves availed by the staff, salary paid to the staff, funds generated by the fees, finance planning etc. These types of systems answer the "what if" question.

(iv)Strategic level System: These support the senior level management to tackle and address strategic issues and long term trends, both inside organisation and the outside world. These answers question like what product should be launched to increase the profit and capture the market and help in long term planning.

Role of information in business

Some of the important implications of the IS in business

Discuss some of the **important implications** of the Information Systems in business. **(PM)**

What are the key **advantages & important implication** of the Proposed Information System for the Company (**May, 15)**

Give some **important advantages** of Information System in business. **(May, 10)**

What is the role of IT in enterprises? **Explain the different levels of managerial activity in an enterprise. (Nov, 15)**

Describe briefly three levels of Management. (Nov, 03)

- ✓ ISs help managers in **efficient decision making** to achieve the organisational goals.
- ✓ An organisation will be **able to survive & thrive** in a highly **competitive** environment **on the strength of a well-designed IS**.
- ✓ ISs help in making **right decision** at the right time.
- ✓ A good IS may help in generating innovative ideas for solving critical problem.
- ✓ Knowledge gathered through ISs may be **utilised by managers in unusual situations**.
- ✓ IS is viewed as a process; it can be **integrated to formulate** a strategy of action or operation.

Three levels of management are briefly discussed below:

- **Strategic level**: Strategic level is defined as a set of management positions that is **concerned with developing of organizational missions, objectives and strategies, directing and managing the organization in an integrated manner.** Decisions made at this level of organization **to handle problems critical to the survival and success** of the organization is called strategic decisions. Strategic level also **establishes a budget framework** under which the various departments will operate.
- **Tactical decisions**: This level lies in the middle of managerial hierarchy. At this level, managers **plan, organize, lead and control the activities** of other managers. Decisions made at this level, called the tactical decisions, are made **to implement strategic decisions.** Tactical decisions are **relatively short,** step-like spot solutions to breakdown strategic decisions into implementable packages**.**
- **Supervisory level**: This is the lowest level in managerial hierarchy. The managers at this level **coordinate the work of others who are not themselves managers**. At supervisory level, managers are **responsible for routine, day-to-day decisions and activities of the organization**, which do **not require much judgment and discretion.** They ensure that specific tasks are carried out effectively and efficiently.

The information can be categorised on the basis of its requirement by the top, middle and lower level management.

Level of management	Constituent	Function	Information requirement
Top Management	Owner/Shareholders, Board of Directors, Managing Director, the chief executive, managers committee	Policy Decision (Introduction of new product line, takeover, merger, acquisition, establishment of new	Strategic Information

		plant)	
Middle Management	Heads of Functions Department(Purchase manager, Production Manager, Sales Manager, financial controller etc)	Implement decision taken by the Top management	Tactical Information
Lower Management	Superintendent, supervisor	Carry out day to day activities	Operational Information

Over view of Underlying Technologies

Modern business uses Information Technology to carry out basic functions including systems for sales, advertisement, purchase, Management reports etc. Briefly discuss some of the IT tools crucial for business growth. **(Nov, 14)**

(i)Business website

(ii)Internet and Intranet

(iii)Software & Package: E.g. ERP Packages

(iv) Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc.

(a) Some of the IT tools crucial for business growth are as follows:

- **Business Website – By having** a website, enterprise/business **becomes reachable to large amount of customers**. In addition, it can also be **used in an advertisement**, which is cost effective and in customer relationship management.
- **Internet and Intranet –** Time and space are **no obstacles** for conducting meeting of **people working in a team from multiple locations**, or with different vendors and companies. Intranet is system that **permits the electronic exchange** of business data within an organization, mostly between managers and senior staff. E-commerce among partners (suppliers, wholesalers, retailers, distributors) using intranets, e-mail etc. provides new platform to the business world for conducting business **in a faster and easier way.**
- **Software and Packages –** DBMS, data warehousing, data mining tools, knowledge discovery can be **used for getting information that plays important role** in decision making that can boost the business in the competitive world. ERP is **one of the latest high-end solutions** that streamlines and integrates operation processes and information flows in the company to **synergize major resources** of an organization.
- **Business Intelligence –** Business Intelligence (BI) refers to **applications and technologies** that are used to collect; provide access and analyze data and information **about companies operations**. Some BI applications are **used to analyze performance or internal operations** e.g. EIS (executive information system), business planning, finance and budgeting tools; while others are used to store and analyze data e.g. Data mining, Data Warehouses, Decision Support System etc. Some BI applications are also used to analyze or manage the human resources e.g. customer relationship and marketing tools.
- **Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc. –**
  Webcam, microphone etc. are **used in conducting long distance meeting**. Use of computer systems, printer, and scanner **increases accuracy, reduce processing times, enable decisions** to be made more quickly and speed up customer service.

Chapter 3: Protection of Information System Control (नियंत्रण)

A legal or official means of regulation or restraint
Control as per ISCA module

Chapter 3: Control is defined as Policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented, detected and corrected. (प्रयाप्त आश्वासन)

Chapter 6:- A control is a system that prevents, detects or corrects unlawful events. Various controls are adopted as per requirement.

SA 315:- "The process designed, implemented and maintained by TCWG, management and other personnel **to provide reasonable assurance about** the achievement of an entity's objectives **with regard** to **reliability** of financial reporting, **effectiveness and efficiency** of operations, **safeguarding** of assets, and **compliance** with applicable laws and regulations.

Control for financial reporting:

Internal control **includes** all of the processes and procedures that management **puts in place** to **help make sure that** its assets are protected and that company **activities are conducted in accordance with the organization's policies and procedures**.

The auditor's objective in an examination of internal control is to form an opinion on the effectiveness of the entity's internal control.

Objective of Controls

To reduce or if possible eliminate the cause of exposure to potential loss.

Discuss information system security and its objective **(RTP -15M)**

What are the major attribute of information security? **(RTP 14N)**

Write a short note on Information System (IS) security objective **(May 2014)**

The objective of information system security is "**the protection of the interests** of those relying on information, and the information systems and communications **that deliver the information**, from harm resulting from failures of confidentiality, integrity, and availability". For any organization, the security objective comprises three universally accepted attributes, which are given as follows:

- **Confidentiality**: Prevention of unauthorised disclosure of information.
- **Integrity**: Prevention of unauthorised modification of information.
- **Availability**: prevention of unauthorised withholding of information.

The relative priority and significance of confidentiality, integrity and availability May vary according to the data within the information system and the business context in which it is used.

कितना असान है.

Preventive controls are intended to prevent the occurrence of an activity that is not consistent with control objectives.

Detective controls are intended to identify errors or unauthorized activities after they have occurred so that corrections can be made in a timely manner.

Entity-level controls are designed **to provide reasonable assurance** that objectives related to the company as a whole are met. Such controls have a pervasive effect on the company's system of internal control.

A **process-level** control pertains to a single activity.

Information Security

What is "Information Security"? State the **core principles** of Information Security. (**MAY 2005)**

Explain in brief information security and its importance. **(May, 04)**

What is "Information Security"? Why is it important in any organization? Explain briefly ***(Nov, 07)***

Security relates to **the protection of valuable assets** against loss, disclosure, or damage. **Securing** valuable assets **from** threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is **commonly understood and implemented by most organizations**. However, security must be **expanded to include logical and other technical safeguards** such as user identifiers, passwords, firewalls, etc. which are not understood nearly as well by organizations as physical safeguards. In organizations where a security breach has been experienced, the effectiveness of security policies and procedures has to be reassessed.

This concept of security applies to all information. **In this context**, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information is **protected against** harm from threats that will lead to its loss, inaccessibility, alteration, or wrongful disclosure. **The protection is achieved** through a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity".

For any organization, the security objective is met when

- information systems are available and usable when required (availability),
- data and information are disclosed only to those who have a right to know it (confidentiality),
- data and information are protected against unauthorized modification (integrity).

Importance of Information Security: In a global information society, where information travels through cyberspace on a routine basis, **the significance of information is widely accepted**. Organizations depend on timely, accurate, complete, valid, consistent, relevant and reliable information. Accordingly, **executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment.**

Today, there are many direct and indirect risks relating to the information systems. These risks have led to gap between the need to protect systems and the degree of protection applied. This gap is caused by:

- **Widespread use of technology;**
- **Interconnectivity of systems;**
- **Elimination of distance, time and space as constraints;**
- **Unevenness of technological changes;**
- **Devolution of management and control;**
- **Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and**
- **External factors such as legislative, legal, and regulatory requirements or technological developments;**

Security failures May result in both financial losses and / or intangible losses such as unauthorized disclosure of competitive or sensitive information.

Threats to information system May **arise** from intentional or unintentional acts **and May come from** internal or external sources. The **threats May emanate** from, among others, technical conditions (program bugs, disk crashes), natural disasters (fires, floods), environmental conditions (electrical surges), human factors (lack of training, errors, and omissions), unauthorized access (hacking), or viruses. **In addition to these**, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) that can potentially result in a loss of management control and oversight are increasing in significance.

Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss or embarrassment caused by security failures.

Information Security Policy

What is meant by information security policy? What are the **components** of a good security policy? **(Nov, 15)**

What is "Information Security"? Why is it important in any organization? Explain briefly (**NOV, 07)**

Security policy defines **acceptable behaviours** and the reaction of the organization **when such behaviours are violated**. The electronic trading, viruses affecting organization's security documents and the misuse of credit cards have increased and **this has augmented the need for security management**. Also, legislation relating to information technology is becoming **more prolific**, with many countries enacting laws on issues such as copyright and software privacy, intellectual property and personal data. These commercial, competitive and legislative pressures require the implementation of proper security policies.

A good security policy should **suggest procedures and policies** that can **prevent loses** and also **help in saving money** and increasing productivity. The security policy **defines ways in which resources in a computer system May be accessed and used**. Security policies might differ depending upon the system under consideration.

Features of Information Security Policy: The security objectives and **core principles provide** a framework **for the first critical step** for any organization-developing a security policy. The security policy should support and complement existing organizational policies. The thrust of the policy statement must be to recognize the underlying value of, and dependence on, the information within an organization. **The information security policy should describe**:

- **Importance** of information security to the organization
- **A statement** from the chief executive officer **in support** of goals and principles **of effective information security**.
- **Specific statements** indicating minimum **standards and compliance requirements** for specific areas.
- Asset **classifications**. a
- Data **security**
- Personnel **security**

- Physical, logical and environment security **Communications security**
- **Legal, regulatory and contractual** security
- System development and maintenance life cycle **requirements** Business continuity planning
- Security **awareness, training and education**
- Security breach **detection and reporting** requirements **Violation** enforcement provision
- **Definitions** of responsibility, accountability for information security and proper separation of duties
- **Reporting responsibilities** and procedures.

A policy is a Principle **to guide** decisions and **achieve rational outcome**. A Policy is a statement of intent and is implemented as a procedure or protocol. Policy is broad guidelines **set by** the Top management in consultation with the expert. The enterprise is expected to follow these guidelines.

For Example, a firm's financial policy may be to keep the debt equity ratio at low level, say, 1 by 1. CFO while taking decision to raise additional finance either through equity or debt he will has to take this policy in mind.

Write short notes on Information System (IS) security objective (**May, 14)**

Information security policy **invariably includes rule intended** to:

- **Preserve & protect** information from any unauthorised modification, access, or disclosure;
- **Limit or eliminate** potential legal liability from employees or third parties; and
- **Prevent waste or inappropriate use** the resources of an organisation.

Tools to implement Policy

Standards: Specifies technologies and methodologies to be used to secure systems. Mandatory होता है

Guidelines: Help in smooth implementation of security policy.

Procedures: It is detailed steps to be followed to accomplish a particular security related task.

Issues to Address

The Information Security Policy of an organization has been defined and documented as given below: "Our organization is committed to ensure Information Security through established goals and principles. Responsibilities for implementing every aspect of specific applicable proprietary and general principles, standards and compliance requirements have been defined. This is reviewed at least once a year for continued suitability with regard to cost and technological changes." Identify the **salient components** that have not been covered in the above policy. **(June, 09)**

What is Information Security Policy? What are the issues it should address? **(May, 13)**

The policy should at least address the following issues;

→ a **definition** of information security,
→ **reason** why infor^{n} security is important to the organisation, and its goals & principles,
→ a **brief explanation** of the security policies, principles, standards, and compliance requirement,
→ definition of all relevant infor^{n} security **responsibilities**, and
→ reference to **supporting documents**.

In the stated scenario of question, the ISMS policy of the given organisation does not address the following issue:

→ a **definition** of information security,
→ **reason** why infor^{n} security is important to the organisation, and its goals & principles,
→ a **brief explanation** of the security policies, principles, standards, and compliance requirement, and
→ reference to **supporting documents**.

Member of security policy

Management member, Technical Group, and Legal Expert.

Give the hierarchy of Information Security Policies and discuss each one of them. **(Nov, 11)**

Infor^{n} security policies and their hierarchy (I, U & AONIC **फिल्म देखने जा रहे हैं**)

- **Information Security Policy**: Provides definition of Information security, its overall objective and the importance applies to all users.
- **User Security Policy:** Set out responsibility and requirement of all IT system users. Provide security term of reference for users, line managers, and system owners.
- **Acceptable Usage Policy:** Set out policy for acceptable use of e-mail and internet service.
- **Organisation Information Security Policy:** Set out group policy for the security of ITS information assets and the IT system processing this information.
- **Network & System Security Policy:** Set out detailed policy for system and network security and applies to all IT department users.
- **Information Classification Policy**: Set out policy for classification of information.

Components of security Policy (RTP 14N))

What should be the **major components** of a good information security policy, as per your opinion? **(May, 12) Same in RTP**

State the **components** of a security policy to protect information system of an organization. **(Nov, 13)**
Briefly outline the **contents** of Information Security policy. **(MAY, 07)**
A good security policy should clearly state the following:

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

Information System Controls

Needs for controls in Information System

Information is a business enabler. Technology has increased the ability to capture, store, analyse, and process tremendous amount of data and information. IS controls procedure may include;

Impact of technology on internal controls

CS तथा CA-करने का PIDAA तु क्या जाने।

- **C:-Competent and Trustworthy Personnel:** Personnel should have **proper skill and knowledge** to discharge their duties. Substantial power is often **vested in the errors responsible** for the computer-based information systems developed, implemented, operated, and maintained within organizations. Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task.
- **S:-Segregation of Duties:** In a manual system, during the processing of a transaction, there are **split between different people**, such that **one person does not process a transaction right from start to finish**. However, in a computerised system, the auditor should also be concerned with **the segregation of duties within the IT department**. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.
- **C:-Comparing Recorded Accountability with Assets:** Data and the assets that the data purports to represent should **periodically be compared to determine** whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. **In a manual system**, independent staff **prepares the basic data** used for comparison purposes. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies o the data being prepared for comparison purposes.
- **A:-Authorization Procedures: In manual systems**, auditors evaluate the adequacy of procedures for authorization of examining the work of employees. **In computer systems**, authorization procedures often are **embedded within a computer program**. For example: In some on-line transaction systems, written evidence of individual data entry authorisation, e.g. a supervisor's signature, may be replaced by computerised authorisation controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
- **P:-Physical Control over Assets and Records:** Physical control over access and records is **critical in both manual systems and computer systems. In the manual systems**, protection from unauthorised access was through the **use of locked doors and filing cabinets**. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. **This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster**. The nature and types of control available have changed to address these new risks.
- **I:-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 the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.
- **D:-Delegation of Authority and Responsibility:** A **clear line of authority and responsibility** is **an essential control** in both manual

and computer systems. In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users. Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

- **A:-Adequate Documents and Records:** In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system. In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available tot trance the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.
- **A:-Adequate Management Supervision:** In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location. In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried our remotely. The Management's supervision and review helps to deter and detect both errors and fraud.

Component of Internal Controls (RTP 14N) (MT 14N)

XYZ Ltd. is a large multinational company with offices in many locations. It stores all its data in just one centralized computer centre. It uses Internal Controls in order to asset safeguarding, data integrity, system efficiency and effectiveness. What could be the **interrelated components** of its Internal Control? Discuss them briefly. ***(Nov, 12)***

Internal controls used within XYZ Ltd. May comprise of the following five interrelated components:

{CERAICA **की** Mother **है}**

- **C**ontrol **E**nvironment:
- **R**isk **A**ssessment:
- **I**nformation and **C**ommunication:
- **C**ontrol **A**ctivities:
- **M**onitoring :

A brief overview of each component is given as follows:

- **Control Environment:** Elements that **establish the control context** in which specific accounting systems and control procedures **must operate**. The control environment is **manifested in management's operating style, the ways authority and responsibility are assigne**d, the functional method of the audit committee, the methods used to plan and monitor performance and so on.
- **Risk Assessment:** Elements **that identify and analyse** the risks faced by an organisation and **the way the risk can be managed.** Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation.
- **Control Activities:** Elements that **operate to ensure** transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.
- **Information and Communication:** Elements, in which **information is identified, captured and exchanged** in a timely and appropriate form to allow personnel to discharge their responsibilities.
- **Monitoring:** Elements that ensure internal controls **operate reliably over time**.

Information Systems Control Technique

Its purpose in the org^n to ensure that the business objectives are achieved and undesired risk event are prevented, detected, and corrected. This is achieved by designing effective information control framework, which comprise policies, procedure, practice and org^n structure that gives reasonable assurance that the business objective will be achieved.

Objectives of Controls:

Some of the critical controls **lacking** in the computerised environment are as follows:

- Lack of management understanding of IS risks and related controls
- Absence or inadequate IS control framework;
- Absence of weak general controls and IS controls;
- Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff;
- Complexity of implementation of controls in distributed computing environments and extended enterprises;
- Lack of control features or their implementation in highly technology driven environments; and
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.

Discuss some of the critical controls **required** in a computerised **environment. (Nov, 14)**

Some of the critical controls **required** in the computerised environment are as follows:

- Management understanding of IS risks and related controls

- ❖ Presence or adequate IS control framework;
- ❖ Presence of weak general controls and IS controls;
- ❖ Awareness and knowledge of IS risks and controls amongst the business users and even IT staff;
- ❖ Implementation of controls in distributed computing environments and extended enterprises;
- ❖ Control features or their implementation in highly technology driven environments; and
- ❖ Appropriate technology implementations or inadequate security functionality in technologies implemented.

Classification of Information Systems Controls

Internal Controls can be classified into **various categories** to illustrate the interaction of various groups in the enterprise and their effect on the information system. Basis of classification are as given below:

→ **Classification on the basis of "Objective of Controls"**
→ **Classification on the basis of "Nature of Information System Resources"**
→ **Classification on the basis of "Audit Functions"**
→ **Classification on the basis of "Functional Nature"**

Classification on the basis of "Objective of Controls" (PDCC)

- **P: Preventive Controls,**
  The broad characteristics of preventive controls are as follows:
  → A clear-cut understanding about the vulnerabilities of the asset;
  → Understanding probable threats; and
  → Provision of necessary controls for probable threats from materializing
- **D: Detective Controls (MT- Nov,14),**
  The main characteristics of such controls are given as follows:
  → Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc;
  → An established mechanism to refer the reported unlawful activities to the appropriate person or group;
  → Interaction with the preventive control to prevent such acts from occurring; and
  → Surprise checks by supervisor.
- **C: Corrective Controls,** & **(RTP-15M)** Do you consider Corrective Controls are a part of Internal Controls? Describe the characteristics of Corrective Controls. **(May, 15) (6 Marks)**
  The main characteristics of the corrective controls are:
  → Minimizing the impact of the threat; Identifying the cause of the problem;
  → Providing Remedy to the problems discovered by detective controls;
  → Getting feedback from preventive and detective controls;
  → Correcting error arising from a problem; and
  → Modifying the processing systems to minimize future occurrences of the incidents.
- **C: Compensatory Controls:-** While designing the appropriate control one thing should be kept in mind - **"The cost of the lock should not be more than the cost of the assets it protects."**

Classification on the basis of "Nature of Information System Resources"

(**E**mpire **P**remier **L**eague)

Explain, briefly, the six categories of controls classified on the basis of **nature of IS resources**. **(Nov, 13)**

❖ Environment Controls, (DHURM - $E^2F^3P^2S^2W^2$)

Discuss different control for environmental exposure. **(MT 15M)**

- D: Documented & Tested Emergency Evacuation
- H: Hand Held fire extinguisher
- U: UPS/Generator
- R: Regular Inspection by Department
- M: Manual Fire alarm
- E: Emergency power off switch
- E: Electronic surge protector
- F: Fire Suppression system
- F: Fire resistance office material
- F: Fire proof, ceiling & floor surrounding the equipment
- P: Prohibition from eating, drinking, smoking within information processing facility

- P: Power lead from two sub-station
- S: Strategically locating computer room
- S: Smoke detector
- W: Water Detector
- W: Wiring placed in electrical conduit & panel

❖ Physical Access Controls, (LOPiLo)

Discuss different means of controlling Physical Access in an organisation. **(RTP -15M)**

- L: Lock on door (Bombay Currency Exchange at Baroda)
  Locks on Doors with respect to Physical Access Control **(Nov, 11)**
  - ✓ **B: Bolting Door Lock**
  - ✓ **C: Cipher Lock**
  - ✓ **E: Electronic Door Lock**
  - ✓ **B: Biometric Door**
- P: Physical Identification Medium (PinPc)
  - ✓ **Pin: Personal Identification Number**
  - ✓ **Pc: Plastic Card/Identification Badge**
- L: Logging on facilities (Easy Money)
  - ✓ **E: Electronic Logging**
  - ✓ **M: Manual Logging**
- O: Other means of controlling physical Access {C^4, DNA test करवाने गया, doctor बोला Virath place जा और SSB मे खाता खुलवा)
  - ✓ **C: Controlled Visitor Access**
  - ✓ **C: Controlled Single Entry Point**
  - ✓ **C: Control of Out of Hours**
  - ✓ **C:Computer Terminal Lock**
  - ✓ **D: Dead Mane Door**
  - ✓ **N: Non-exposure of sensitive material**
  - ✓ **A: Alarm System**
  - ✓ **V: Video Camera**
  - ✓ **P: Perimeter Fencing**
  - ✓ **S: Security Guard**
  - ✓ **S: Secured Report/ Documentation Distribution Cart**
  - ✓ **B: Bonded Personnel**

❖ Logical Access Controls, (MONU UA)

- **M: Mobile Computing Related Control**
- **O: Operating System Access Control**
- **N: Network Access Control**
- **U: User Access Management**
- **U: User Responsibilities**
- **A: Application & Monitoring System Access Control**

Classification on the basis of "Audit Function":

❖ Management Control (TIPS presents DOS- Q)

- **T: Top Management**
- **I: IS Management**
- **P:Programming Management**
- **S: System Development Management**
- **D: Data Administration**
- **O: Operation Management**
- **S: Security Administration**
- **Q: Quality Assurance Management**

❖ Application Control (Personal Computer BIDO)

- **P: Processing Control**
- **C: Communication Control**

- **B: Boundary Control (RTP)**
- **I: Input Control**
- **D: Database Control**
- **O: Output Control**

Classification of Controls based on "function" (Indian Medical Association)

When **reviewing a client's control systems**, the auditor will be **able to identify three components** of internal control. Each component is aimed at achieving different objectives. These controls are given as follows:

(i) **Internal Accounting Controls:** The Controls which are intended to safeguard the client's assets and ensure the reliability of the financial records are called internal accounting controls.

(ii) **Management Controls:** These are concerned with ensuring efficiency and compliance with management policies, including the operational controls. **&**

(iii) **Administrative Controls:** These deals with the day-to-day operations, functions and activities to ensure that the operational activities are contributing to business objectives. **.**

Brief explanation of above Classification

Physical Access Controls:

Designed to protect the organisation from UNAUTHRISED access or prevent illegal entry. Allows access only to Authorised persons. Physical and Environment Protection:

Physical Access Issues and Exposures:

(a)Possible Perpetrator

(b)Access Control Mechanism (ACM):

Discuss the three processes of Access Control Mechanism, when a user requests for resources. **(Nov, 09)**

An ACM associate with identified, authorised users the resources they are allowed to access & action privileges. The ACM processes the user request for the resource in three steps. They are:

→ Identification,

→ Authentication, &

→ Authorisation.

The access control mechanisms operate in the following sequence:

1. The users have to identify themselves, thereby indicating their intent to request the usage of system resources,
2. The users must authenticate themselves and the mechanism must authenticate itself, and
3. The users request for specific resources, their need for those resources and their areas of usage of these resources.

   The mechanism accesses
   (a) previously stored information about users,
   (b) the resources they can access, and
   (c) the action privileges they have with respect to these resources.

The mechanism verifies this information against the user entries and it then permits or denies the request.

Identification and Authentication: Users identify themselves to the access control mechanism by providing information such a name, account number, badge, plastic card, finger print, voice print or a signature. To validate the user, his entry is matched with the entry in the authentication file. The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.

(c)Authorisation: There are two approaches to implementing the authorization module in an access control mechanism:

- **Ticket Oriented Approach of authorisation:** In this approach the access control mechanism assigns the users a ticket for each resource they are permitted to access. Ticket oriented approach operates via a row in the matrix. Each row along with the user resources holds the action privileges specific to that user
- **List Oriented Approach of authorisation:** In this approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

Locks on Doors with respect to Physical Access Control **(Nov, 11)**

Locks on Doors with respect to physical access control: Different types of locks on doors for physical security are discussed below:

© **Cipher Locks (combination Door Locks):** The Cipher Lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit

number sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds. Cipher Locks are used in low security situations or when a large number of entrances and exits must be usable all the time. More sophisticated and expensive cipher locks can be computer coded with a person's handprint. A matching handprint unlocks the door.

© **Bolting Door Locks:** A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry the keys should not be duplicated.

© **Electronic Door Locks:** A magnetic or embedded chip based plastics card key or token May be entered into a sensor reader to gain access in these systems. The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism.

© **Biometric Door Locks:** These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

Logical Access Controls

System Based Mechanism

Types of Logical Access Path:

- **Online Terminals**: To access OT, a user has to provide a valid login-ID and password.
- **Dial-up Ports:** Using it, user at one location can CONNECT remotely to another computer present at unknown location via a telecommunication media.
- **Telecommunication Network:** In a TN, a number of computer terminals are linked to the host computer through network or TL.

Issues and Revelations related to Logical Access:

→ **Technical Exposure,**
→ **Asynchronous Attack, &**
→ **Loss of exposures.**

Technical Exposure: it includes unauthorised implementation or modification of data and software. (DB TW RST)

1. **Data Diddling:** Change of data before or after they are entered into the system.
2. **Bomb:** it is a piece of bad code deliberately planted by an insider or supplier of programmer.
   - ✓ **Time Bomb:** It causes perverse activity, such as, disruption of computer system, modification or destruction of stored information.
   - ✓ **Logic Bomb**: It is activated by combination of events.
3. **Trojan Horse:** Malicious programs that are hidden under any authorised program. It may change or steal the password or modify records in protected file or allow illicit users the use the system. It get activated only if the illicit program is called explicitly. Not damage the host program & not copy itself to other software in the same or other systems. (**RTP 14N**)
4. **Worms**: Not require host program to relocate itself. Copy itself to another machine on the network. Standalone program & can be detected easily.
5. **Rounding Down**: rounding of small fractions of a denomination and transferring it into an authorised account.
6. **Salami Technique**: slicing of small amounts of money from a computerised transaction or account. , and
7. **Trap Doors:** it allows insertion of unauthorised logic.

Asynchronous Attack: (QPM) (**RTP 14N**)

Where data can be moved asynchronously (DaWi PiShu)

- ➢ **Data leakage:** Leaking information out of the computer by means of dumping files to paper or stealing computer record & tape.
- ➢ **Wire tapping:** Spying on information being transmitted over TN.
- ➢ **Piggybacking**: , and
- ➢ **Shutting down of compute/DOS**:

Computer Crime Exposure (Loss):

'Crimes are committed by using computer and can damage the reputation, morale and even the existence of an organisation'. What are the problems do you think that any organisation can face with the result of computer crimes? **(Nov, 15)**

- **Financial loss,**
- **Legal Repercussion,**
- **Loss of Credibility,**
- **Blackmail,**
- **Disclosure of confidential, sensitive or embarrassing information, and**
- **Sabotage.**

Controls for remote and distributed data processing: (QPM)

Explain briefly major ways to control remote and distributed data processing in the new Web Application. **(May, 15)**
Distributed & remote application can be controlled in many ways. Some of these are given as follows;

→ **Remote access** to computer & data files **through the network** should be **implemented**;

→ Having **a terminal lock** can assure physical security;

→ **Application** that can be remotely accessed via modems & other device should be **controlled appropriately**;

→ **Terminal** & computer **application at the remote locations** should be **monitored** carefully & frequently for violation;

→ In order to **prevent unauthorised user** from the accessing the system, there should be **proper control mechanisms** over system documentation and manual;

→ **Data transmission** over remote locations should be **controlled**. The location which sends data should **attach needed control information** that helps receiving location to verify the genuiness and integrity;

→ When **replicated copies** of file exist **at multiple locations** it must be ensured that **all identical copies contain the same information** & checks are also implemented to ensure that duplicate data does not exist.

Cyber Frauds

On the basis of the functionality, cyber frauds are of two types;

- **Pure Cyber Fraud**: Only exist in cyber world, and
- **Cyber Enabled Fraud**: Committed in physical world also, but with the use of technology; the size, scale and location of fraud change.

Cyber Attack:

Describe the various threats to the computerized environment due to cyber crimes. **(May, 14)**
(a)**Phishing**: The act of attempting to acquire information by masquerading as a trustworthy entity in the EC.
(b)**Network Scanning**: A process to identify ACTIVE HOST of a system, for the purpose of getting information about IP addresses etc.
(c)**Virus/malicious Code**
(d)**Spam**: E-mailing same message to every one on one or more USE NET group is termed as spam.
(e)**Website Compromise**: Website defacement.
(f)**Others**: (Crackers, Eavesdropping, E-mail forgery, E-mail threat, Scavenging)

Technique to commit cyber Frauds (RTP-15M)

Define the following computer Fraud and Abuse technique:

- ✓ Hacking
- ✓ Logic time bomb
- ✓ Piggy backing
- ✓ Spamming:It refers to a situation where the same message is e-mailed to everyone on one or more Usenet news groups or LISTSERV lists.
- ✓ Data diddling. **(MAY 2006)**

Discuss some of the major techniques to commit cyber frauds. **(MT 14N)**
[3D और 3S को पता है PP & HIC का झगडा जो LMR के Top Floor मे किएं थे]

- **D: DOS attacks:** An action or series of actions that **prevents access** to a system by ITS AUTHORISED user; causes **delay of its time-critical operation**; or prevents any part of the system from functioning.
- **D: Data leakage**
- **D: Data diddling**: Changing data **before, during or after** it is entered into the system in order **to delete alter or add** key system data is known as data diddling.
- **S: Super Zapping**: Unauthorised use of special system programs to **bypass regular system controls** and perform illegal acts.
- **S: Social Engineering:** Perpetrator tricks an employee into **giving out the information needed to get into the system**.
- **S: Scavenging: Gaining access** to confidential information **by searching corporate records** is termed as scavenging. Scavenging methods range from searching for printouts or carbon copies of confidential information to scanning the contents of computer memory.
- **P: Password Cracking**: Intruder **penetrates** a system's DEFENSE, STEALS the file containing valid password, **decrypt** them and then **uses** them to gain access to system resources.
- **P: Piggybacking:** It refers to **tapping into a telecommunications** line and **latching on to a legitimate user** before he logs into the system; legitimate user unknowingly carries perpetrator into the system.
- **H: Hacking**: It refers to **unauthorized access** to and use of computer system usually **by means of a personal computer and telecommunication network.**

- **I: Internet terrorism:** Using internet to **disrupt** electronic commerce and **to destroy** company and individual communications is referred as internet terrorism.
- **C: Cracking: Unauthorized access** to and use of computer systems, usually by means of a personal computer and a telecommunications network is called cracking. Crackers are hackers **with malicious intentions**.
- **L: Logic Time Bomb:** It refers to the program that **lies idle** until some specified circumstance or a particular time triggers it. Once triggered, the bomb **sabotages** the system by destroying programs, data or both.
- **M: Masquerading or Impersonation**: Under this technique, perpetrator **gains access** to the system **by pretending to be an authorized user** and enjoys same privileges as the legitimate user. Fraud messages can be sent to the receiver by using legitimate users identity and thus can prove to be harmful.
- **R: Round Down**
- **T: Trap door**

Define the following computer fraud and abuse technique:

- War diling: It relates to programming a computer search for an idle modem by dialing thousands of phone lines. Perpetrator enters the system through idle modem, captures the personal computer attached to the modem, and gain access to the network to which the personal computer is attached.
- Scavenging
- Cracking
- Internet terrorism
- Masquerading. **(May, 08)**

Impact of cyber fraud on enterprise

Discuss computer crime exposure in brief. **(MT 14N)**

What are the **repercussions** of cyber frauds on an enterprise? **(Nov, 14)** (File LoDiS)

(1) Financial Loss:
(2)Legal Repercussion:
(3)Loss of credibility or competitive edge:
(4) Disclosure of confidential information:
(5)Sabotage:

The repercussions of cyber frauds on an enterprise can be viewed under the following dimensions:

→ **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, 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 the Information Technology Act, 2000, 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.

→ **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack May expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.

→ **Sabotage:** The above situation May lead to misuse of such information by enemy country.

Application Controls/User controls

Software Applications require interface between user and the business functions. Discuss **User Controls** describing various types of controls to be exercised to achieve system effectiveness and efficiency**. (May, 15)**

Application represents an interface between the user and the business functions. User's controls that are to be exercised for system effectiveness and efficiency. **(P**ersonal **C**omputer **BIDO)**; (**RTP 14N**)

→ **B: Boundary Controls:** Comprises the components that establish the interface between the user and the system
→ **I: Input Controls:** Comprises the components that capture, prepare, and enter commands and data into the system.
→ **P: Processing Controls:** Comprises the components that perform decision making, computation, classification, ordering, and summarization of data in the system.
→ **O: Output Controls:** Comprises the components that retrieve and present data to users of the system.
→ **D: Database Controls:** Comprises the components that define, add, access, modify, and delete data in the system.
→ **C: Communication Control:** Comprises the components that transmit data among subsystems and systems.

Boundary Controls:

You are selected by UVW Limited to review and strengthen Software Access Control mechanism for their Company. Prepare a report on the need of boundary controls enlisting major boundary control techniques to be implemented by them. **(May, 15)**

The company UVW Limited intends to review and strengthen its Software Access Control mechanism. To achieve this objective, the Boundary controls can be put in place that will establish interface between the user of the system and the system itself. The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access and thus are the line of control for intruders to gain access to UVW Company's asset. The access control mechanism has three steps of Identification, Authentication and Authorization with respect to the access control policy implemented. The user can provide three factors of input information for the authentication process and gain access to his required resources.

What **boundary control techniques** should be used **in user control**? **(May, 13)**

Discuss boundary control and their technique. **(MT 15M)**

Major controls of the BS are the ACM. ACM links the authentic users to the authorised resources, they are permitted to access. 3 steps are identification, authentication and authorisation.

Major controls are (**P**rivate **C**ompany BIP)

- **P: Password**: User identification by an authentication mechanism with personal characteristic such as name, DOB, E Code, function, designation or a combination of two or more can be used as a password BC.
- **C: Cryptography**: Program for transforming into cipher text that are useless to anyone, who does not possess the authentication to access the respective system resources.
- **B: Biometric device**:- Biometric identification e.g. thumbs and/or finger impression, eye retina etc. are also used as boundary control techniques.
- **I: Identification Card**: It used to store information required in an authentication process. Cards are to be Controlled through the application for a card, preparation of the card, issue, use, return or termination.
- **P: PIN**: PIN, similar to a password assigned to a user by an institution, is a random number stored in its database independent to a user identification details, or a customer selected number.

Input Controls:

These controls are responsible for ensuring the **accuracy and completeness** of data and instruction input into an application system. It might be necessary **to reprocess input data** in the event, master files are lost, corrupted, or destroyed. Input controls are divided into the following broad classes: (**S**abita **D**evi **V**aluable **B**habhi)

1. **Source Document controls,**
2. **Data Coding Controls,**
3. **Validation Controls.**
4. **Batch Controls,**

(1)Source Document Controls: Where physical source document is used to initiate transaction then the following controls needs to be in place. SD fraud can be used to remove assets from the organisation. These control procedures are used to account for each source document.

- **Use pre-numbered source document:** SD Come pre-numbered from the printer with sequential number on each document. It enables **accurate accounting of document usage** & provide audit trail for tracing transaction through accounting record.
- **Use Source document in sequence:** Source documents should be distributed to the users and used in sequence. Require adequate physical security maintained over the source Document inventory at the user site**.**
- **Periodically audit source documents:** Missing document should be identified by reconciling sequence number. Periodically, the auditor should compare the source document used to the date with those remaining in inventory + those avoided due to error. Documents not accounted for should be reported to management.

(2)Data Coding Controls: Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors, which are as discussed below: Transcrip की पत्नि Transpo का झागडा चल रहा है वो कहता है All Time Sex करते, वो कहती है Sleep Now Multi at Nights.

→ **Transcription Errors:** Addition, Truncation, and Substitution Errors.

→ **Transposition Errors**: Single, and Multiple transposition errors.

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

What is the **significance** of input validation control? Describe briefly three different levels of input validation controls used in computerized information system. **(MAY 2006)**

There are three levels of input validation controls; (Field मे Rose Flower है)

- **Field interrogation,**
- **Record interrogation, and**
- **File interrogation**.

Field interrogation: Discuss some types of Field interrogation as a validation control procedure in an EDP set up.**(Nov, 06)**
It involves **programmed procedures** that examine the characters of the data in the field. Various field checks used to ensure data integrity are given as under (**P**apu Lal V-CA)

- **P: Picture Checks**: These check against entry of incorrect/invalid characters into processing.
- **L: Limit Check:** The field is checked by the program to ensure that its values lies within certain predefined limit.
- **V: Valid Code Checks:** Checks made against **predetermined transaction codes**, tables or order data **to ensure that input data are valid**. Predetermined codes are ether embedded **in the programs or stored in files**.
- **C: Check Digit:** It is an extra digit that is added to the code when it is originally assigned. It allows integrity of code to be established during the subsequent processing.
- **A: Arithmetic Checks:** Simple Arithmetic is performed **in different ways** to validate the result of **other computation** of the value selected data fields.
- **Cross check**: It may be employed **to verify fields** appearing in different files to check that the result tally.

Record interrogation: (Raj Vihari Shastri)

- **Reasonableness check:** Whether the value **specified** in the field is reasonable for that particular field?
- **Valid Sign:** The content one field determine which sign is valid for a numeric field.
- **Sequence Check**: If **physical record** follows a required order matching with **logical record**.

File Interrogation: (Veena initially dedicated श्री bargaining of figure maintenance product).

→ **V: Version Usage**: Proper version of a file should be used for processing the data correctly. It should be ensured that only most current file us processed.
→ **I: Internal and external labelling**: Labeling of storage media is important **to ensure that the proper file is loaded for processing.** External Labeling is used where there is manual process for loading file. Automated tape loader system is used, then, **internal** Labeling is important**.**
→ **Data file security**: Unauthorised access to data file should be prevented, to ensure its CIA.
→ **B: Before and after image and logging**: The application may **provide for** reporting before and after images of the transaction. These images combined with the logging of events enable **re-constructing** the data file back to its last state of integrity, after which application can **ensure that the incremental transaction rolled back or forward.**
→ **F: File updating and maintenance authorisation**: Sufficient control should exist for file updating and maintenance **to ensure that the stored data are protected**. The access restriction may be either be part of the application program or of the overall system access restrictions.
→ **P: Parity Check**: When program or data is transmitted, **additional controls are needed**. Transmission errors are controlled primarily by detecting errors or correcting codes.

Output controls:

As an IS auditor, what are the output controls required to be reviewed with respect to application controls? **(Nov, 14)**
As an IS auditor, what are the **output controls** required to be reviewed with respect **to application controls**? **(May, 14)**
Discuss various output controls in detail. **(MT-Nov.14)**
What is the scope of **output control** of **an application system**? Suggest various types of output controls which are enforced for confidentiality, integrity and consistency of output. **(May, 13)**
These controls ensure that the **data delivered to users will be presented, formatted and delivered in a consistent and secured manner**. Output controls have to be enforced both in a batch-processing environment as well as in an online environment. Various Output Controls are given as follows: (**S**tatutory **L**iquidity **R**atio & **C**orporate **S**ocial **R**esponsibility)

- **S: Storage and Logging of critical items:** Pre-printed stationery should be **stored securely** to prevent unauthorized destruction or removal and usage. Only authorized persons should **be allowed access** to stationery supplies such as security forms, negotiable instruments, etc.
- **L: Logging of output program execution:** When **programs** used for output of data **are executed**, these should be **logged and monitored**; otherwise confidentiality/integrity of the data may be **compromised**.
- **R: Retention controls:** Retention controls consider the **duration for which outputs should be retained** before being destroyed. Retention control requires that a **date** should be **determined** for each output **item produced**. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.
- **C: Control over printing:** Outputs should be made **on the correct printer** and it should be ensured that **unauthorized disclosure** of information printed does **not take place**. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- **Spooling/Queuing:** "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user is able to continue working, while the print operation is getting completed. When a file is to be

printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is then "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer; this should not be subject to unauthorized modifications.

- **R: Reporting distribution and collection controls:** Distribution of reports should be **made in a secure way** to prevent **unauthorized disclosure** of data. It should be **made immediately** after printing to ensure that the time **gap** between generation and distribution is **reduced**. A log should be maintained for reports that were generated and to whom these were distributed.

Database controls:

Protecting the **integrity of the database** when application software acts **as an interface between** the user and database, are called update control and report controls.

Update Control: Major update controls (Sequence Ensure Process to be Maintained)

- **Sequence check between transaction and master file: Synchronisation and correct** processing transaction between the MF and TF is **critical to maintain** the INTEGRITY of up-dation, insertion or deletion of records in the MF with respect to T Records. **If errors,** in this stage are overlooked, **it leads to corruption of the critical data**.
- **Ensure all records on files are processed:** While processing, the TF records **mapped to the** respective MF, **and** the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.
- **Process multiple transactions for a single record: Multiple** transactions can **occur** based on a single master record (e.g. dispatch of a product to different distribution centers). Here, **the order in which transactions** are processed against the product master record **must be done based on a sorted transaction codes**.
- **Maintain a suspense account:** When **mapping between** the master record to transaction record **results in a mismatch** due to failure in the corresponding record entry in the master record; **then these transactions are maintained in a suspense account**. **A non-zero balance** of the suspense accounts **reflects the errors to be corrected**.

Report controls: Major Report controls are given as follows:

- **Standing data:** Application programs use **many internal tables to perform various functions**. **Maintaining integrity** of the table is critical within an organisation. **Any changes or errors** in these tables would have **an adverse effect** on the organizations basic functions. **Periodic monitoring** of these internal tables by means of manual check or by calculating a control total **is mandatory**.
- **Print-Run –to- Run controls total:** It helps **in identifying** errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.
- **Print suspense account entries**: Similar to the update controls, the suspense account entries are to be **periodically monitors** with the respective error file and action taken on time.
- **Existence/Recovery Controls:** The Back-up (BU) and recovery strategies (RS) together ENCOMPASS the control required to restore failure in database. BU strategies are implemented using PRIOR VERSION and LOGs OF TRANSACTION or changes to DB. RS involve ROLL-FORWORD (current state DB from previous version) or ROLL-BACK (previous state DB from current version).

Processing Controls

The processing sub-system is **responsible for** computing, sorting, classifying, and summarizing data. **Its major components** are the Central Processor in which programs are **executed**, the real or virtual memory in which **program instructions and data** are **stored**, the operating system that **manages system resources**, and the application programs that **execute instructions** to achieve specific user requirements. (PVR-Delhi)

- **Processor Controls**
- **Virtual Memory Controls**
- **Real Memory Controls:**
- **Data Processing Controls:**

(I)Processor Controls: The processor has **three components**: (a) A Control unit, which fetches programs from memory and determines their type; (b) an Arithmetic and Logical Unit, which performs operations; and (c) Registers, that are used to store temporary results and control information. **Four types of controls** that can be used **to reduce expected losses** from errors and irregularities **associated with Central processors** are

→ **Error Detection And Correction:** Occasionally, processors might **malfunction**. The **causes** could be design errors, manufacturing defects, damage, fatigue, electromagnetic interference, and ionizing radiation. **Various types of error detection and correction strategies must be used.**

→ **Multiple Execution States:** It is important to determine the **number of and nature** of the execution states **enforced by the processor.** This helps auditors to determine **which user processes will be able to carry out unauthorized activities**, such as

gaining access to sensitive data maintained in memory regions assigned to the operating system or other user processes.

→ **Timing Controls:** An operating system might **get stuck in an infinite loop**. In the absence of any control, the program will **retain use of processor** and prevent other programs from **undertaking their work**.

→ **Component Replication:** In some cases, **processor failure** can result in significant losses. **Redundant processors** allow errors to be **detected and corrected**. If processor failure is permanent in multicomputer or multiprocessor architectures, the system might **reconfigure itself** to isolate the failed processor.

(II)Real Memory Controls: This comprises the **fixed amount of primary storage** in which programs or data must **reside** for them to be **executed or referenced** by the central processor. Real memory controls **seek to detect and correct errors** that occur in memory cells and **to protect areas of memory assigned** to a program from illegal access by another program.

(III)Virtual Memory Controls: Virtual Memory **exists when the addressable storage space is larger** than the available real memory space. To achieve this outcome, a control mechanism must be in place **that maps virtual memory addresses** into real memory addresses.

(IV)Data Processing Controls

These perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. (FREE - ₹)

- F: Field Initialization: Data **overflow can occur**, if records are **constantly added** to a table or if fields are **added to a record** without initializing it, i.e. setting all values to zero/blank before inserting the field or record.
- R: Run to run Totals,: These help **in verifying data** that is subject to process through different stages. If the current balance of an invoice ledger is ` 150,000 and the additional invoices for the period total ` 20,000 then the total sales value should be ` 170,000. A specific record probably the last record can be used to maintain the control total.
- E: Edit Check: It is **similar to data validation controls** can also be used as at the processing stage t**o verify accuracy and completeness of data.**
- E: Exception Report: Exception reports are generated **to identify errors** in the data processed. Such exception reports give the **transaction code** and **why** a particular transaction was **not processed** or what is the error in processing the transaction. For example, while processing a journal entry if only debit entry was updated and the credit entry was not updated due to the absence of one of the important fields, then the exception report would detail the transaction code, and why it was not updated in the database.
- **Reasonableness Verification**: 2 or more fields can be **compared and cross verified** to ensure their correctness. For example, the statutory percentage of provident fund can be calculated **on the gross pay** amount to verify if the provident fund contribution deducted is accurate.

Communication Controls

Three major types of exposure arise in the communication subsystem:

→ Transmission **impairments** can cause difference between the **data sent and the data received**;

→ Data can be **lost or corrupted** through component failure; and

→ A **hostile party** could seek to subvert data that is transmitted through the subsystem.

These controls **discusses exposures** in the communication subsystem, 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.

(**PLF LTd. का Construction का Innovative है।**)

© **P:-Physical Component Controls:**
(CPT- M)
  → **M:-Modem**
  → **C:-Communication line**
  → **P:-Port Protection Device**
  → **T:-Transmission Media**

© **L:-Line error control:**

© **F:-Flow Controls:**

© **L:-Link Controls:**

© **T: -Topological Controls:**

© **C:-Channel Access Controls:**

© **I:-Internetworking Controls:**
  ✓ **Gateway**
  ✓ **Bridge**

- ✓ **Router**

(A) **Physical Component Controls**: These controls incorporate features **that mitigate the possible effects of exposures**. An overview of how **physical components can affect communication** subsystem reliability**.**

(i)Transmission Media: It is **a physical path** along which a signal can be transmitted between a sender and a receiver. It is of two types:

→ Guided/Bound Media in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber.

→ In Unguided Media, the signals propagate via free-space emission like – satellite microwave, radio frequency and infrared.

(ii)Communication Lines: The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.

(iii)Modem:

- ❖ **Increases the speed** with which data can be **transmitted** over a Protection of Information Systems *communication line.*
- ❖ Reduces the number of line errors that arise through distortion if they use a process called equalization.
- ❖ Reduces the number of line errors that arise through noise.

(iv)Port Protection Devices: Used to **mitigate exposures associated with dial-up access** to a computer system. The port-protection device **performs various security functions** to authenticate users.

(v)Multiplexers And Concentrators:

- These allow the band width or capacity of a communication line to be used more effectively.
- These share the use of a high-cost transmission line among many messages that arrive at the multiplexer or concentration point from multiple low cost source lines.

(B)**Line Error Control**: Whenever data is transmitted over a communication line, recall that it can be **received in error** because of **attenuation distortion**, or **noise that occurs on the line**. **These errors must be detected and corrected**.

- ❖ **Error Detection:** The errors can be **detected** by either using **a loop** (echo) check or building some form **of redundancy** into the message transmitted.
- ❖ **Error Correction:** When line errors have been **detected**, they must then be corrected using either **forward error correcting codes** or **backward error correcting codes.**

(C)Flow Controls: Flow controls are needed because **two nodes** in a network can **differ** in terms of the **rate at which they can send**, received, and process data. For example, a main frame can transmit data to a microcomputer terminal. The microcomputer cannot display data on its screen **at the same rate** the data arrives from the main frame. Moreover, the microcomputer will have **limited buffer space**. Thus, it cannot continue to receive data from the mainframe and to store the data in its buffer **pending display of the data on its screen.** Flow controls will be used, therefore, **to prevent the mainframe swamping the microcomputer and, as a result, data is lost.**

(D)Link Controls: In WANs, line error control and flow control are important functions **in the component** that manages the link between two nodes in a network. The link management components mainly use **two common protocols** HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

(E)Topological Controls: A communication network topology **specifies the location of nodes** within a network, **the ways in which these nodes will be linked**, and the data **transmission capabilities** of the links between the nodes. Specifying the **optimum topology** for a network can be a problem of immense complexity**.**

→ **Local Area Network Topologies:** LAN tend to have **three characteristics**: (1) they are **privately owned** networks; (2) they provide high**-speed communication** among nodes; and (3) they are **confined to limited geographic areas** (for example, a single floor or building or locations within a few kilometers of each other). They are **implemented** using **four basic types of topologies**: (1) bus topology, (2) Tree topology, (3) Ring topology, and (4) Star topology. Hybrid topologies like the star-ring topology and the star-bus topology are also used.

→ **Wide Area Network Topologies:** WAN have the following **characteristics**:

- they often encompass components that are **owned by other parties** (e.g. a telephone company);
- they provide relatively **low-speed communication** among nodes; and o they span large geographic areas

With the **exception of the** bus topology**, all other topologies** that are used **to implement LANs** can also be used **to implement WANs**.

(F)Channel Access Controls: Two different nodes in a network **can compete to use a communication channel**. Whenever the possiblility of contention for the channel exists, some type of channel **access control technique must be used**. These techniques fall into two classes: Polling methods and Contention methods.

- ✓ **Polling:** Polling (non contention) techniques **establish an order** in which a node can **gain access to channel capacity**.
- ✓ **Contention Methods:** Using contention methods, nodes in a network **must compete with each other** to gain access to a channel. Each node is **given immediate right of access** to the channel. Whether the node can use the channel successfully, however, **depends on the actions of other nodes connected to the channel**.

(G) Internetworking Controls: Internetworking is **the process of connecting** two or more communication **net-works together** to allow the **users** of one network **to communicate with the users of other networks**. The networks connected to each other might or might not **employ the same underlying hardware-software platform.** Three types of devices are used **to connect sub-networks** in **an internet** are

Bridge: A bridge connects **similar local area networks** (e.g. one token ring network to another token ring network).

Router: A router performs **all the functions of a bridge**. In addition, it can **connect heterogeneous local areas networks** (e.g. a bus network to a token ring network) and direct network traffic over the fastest channel between two nodes that reside in different sub-networks (e.g. by examining traffic patterns within a network and between different networks to determine channel availability.)

Gateway: Gateways are the **most complex of the three network connection devices**. Their primary function is **to perform protocol conversion to allow different types of communication** architectures to communicate with one another. The gateway maps the functions performed in an application on one computer to the functions performed by a different application with similar functions on another computer.

Management Control (TIPS presents DOS- Q)

- **T:** Top Management: Top management must ensure that information systems function is well managed. It is responsible primarily for long – run policy decisions on how Information Systems will be used in the organization.
- **I:-**IS Management: IS management has overall responsibility for the planning and control of all information system activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.
- **P:-**Programming Management: It is responsible for programming new system; maintain old systems and providing general systems support software.
- **S:-**System Development Management: Systems Development Management is responsible for the design, implementation, and maintenance of application systems.
- **D:-**Data Administration: Data administration is responsible for addressing planning and control issues in relation to use of an organization's data.
- **O:-**Operation Management**:** It is responsible for planning and control of the day-to-day operations of information systems.
- **S:-**Security Administration**:** It is responsible for access controls and physical security over the information systems function.
- **Q:-**Quality Assurance Management: It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.

Controls over Data Integrity and Security

When data is stored, whether created, received or amended, it should always be classified into an appropriate sensitivity level. (**QPM**)
What do you understand by classification of information? Explain different classifications of information**. (Nov, 08)**
As a member of IS Steering committee, how do you classify the information for better integrity and security? **(Nov, 15)**

Major data classification can be; (Hindustan Time PIPer)

Information classification does **not follow any predefined rules**. It is **a conscious decision** to assign a certain sensitivity level to information **that is being created, amended, updated, stored, or transmitted**. The sensitivity level **depends upon the nature of business in an organization and the market influence.**

The classification of information **further determines the level of control and security requirements**. Classification of information is **essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality**. When data is stored, whether received, created or amended, it should **always be classified into an appropriate sensitivity level** to ensure adequate security.

For many organizations, a very simple classification criterion is given as follows:

→ **T: Top secret:** Highly **sensitive internal information** (e.g. pending mergers or acquisitions; investment strategies; plans or designs) that could **seriously damage** the organization **if such information were lost or made public**. Information classified as Top Secret information has **very restricted distribution** and **must be protected at all times**. **Security at this level should be the highest possible.**

→ **H: Highly confidential:** Information that, **if made public or even shared around** the organization, could **seriously impede the organization's operations** and is **considered critical** to its ongoing operations. Information would **include** accounting information, business plans, sensitive customer information of banks, solicitors and accountants, patient's medical records and similar highly sensitive data. Such information should **not be copied or removed from** the organization's operational control without specific authority. **Security at this level should be very high**.

→ **P: Proprietary:** Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications **that define the way in which the organization operates**. Such information is normally **for proprietary use to authorized personnel only**. **Security at this level should be high**.

→ **I: 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**. Examples would include, internal memos, minutes of meetings, internal project reports. **Security at this level should controlled but normal.**

→ **P: Public Document:** Information **in the public domain**; annual reports, press statements etc.; which has been **approved for public use**. **Security at this level should minimal**.

Data integrity controls:

"Once the information is classified on various levels, the organization has to decide about the implementation of different data integrity controls." Do you agree? If yes, explain about data integrity and its policies**. (Nov, 10)**

Yes, we agree with the statement given in the question.

Data integrity is a reflection of the accuracy, correctness, validity and currency of the data. The primary objective in ensuring integrity is to protect the data against erroneous input from authored users.

Major Data integrity control (DOSI-DO लोग हैं)

- **Data Processing and Storage Controls:**
- **On-line Data Entry Controls:**
- **Source Data Controls:**
- **Input Validation Controls:**
- **Data Transmission Controls:**
- **Output Controls:**

Data Integrity Policy (RTP, 14N) (QPM)

What are the major data integrity policies you would suggest? **(Nov, 14)**

Major data integrity policies are given as under: **{VOSD- Q D}**

→ **V: Virus Signature Updating**: It must be updated automatically when they are made available from vendor through enabling of automatic updates.

→ **O: Offsite Backup Storage**: Backups must be sent offsite for permanent storage.

→ **S: Software Testing:** All software must be tested in a suitable tats environment before installation in production environment.

→ **D: Division of Environment:** The division of environments into Development, Test, and Production is required for critical systems.

→ **Q: Quarter-End and Year End Backup**: Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes

→ **D: Disaster Recovery:** A comprehensive DRP must be used to ensure continuity of corporate business in the event of an outage.

Date Security

Controls Technique

Differentiate between General and Application controls. Also mention the broad categories into which the first can be subdivided. **(Nov, 06)**

General controls apply to a wide range of exposures that systematically threaten the integrity of all applications processed within CBIS environment. **Application controls** are focused on exposures associated with specific systems such as payroll, accounts receivable etc. These controls help to ensure the completeness and accuracy of transaction processing, authorization, and validity.

General controls can be subdivided under following headings:

→ **Operating system controls**

→ **Data managements Controls**
→ **Management controls**
→ **Organizational structure controls**
→ **Systems development controls**
→ **Computer Centre security controls**
→ **Internet and intranet controls**
→ **Personal computers control.**
→ **Financial Controls**

Data Management Controls

These Controls fall in two categories:

- **Access Control**, and
- **Backup Control.**

Access Controls: Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner:

→ User Access Controls through passwords, tokens and biometric Controls; and
→ Data Encryption: Keeping the data in database in encrypted form

Back-up Controls: Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases.

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are given as follows:

→ **Dual recording of data***:* Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
→ **Periodic dumping of data**: This strategy involves taking a periodic dump of all or part of the database. The database is saved at a point in time by copying it onto some backup storage medium – magnetic tape, removable disk, Optical disk. The dump may be scheduled.
→ **Logging input transactions***:* This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump. In case of complete database failure, the last dump is loaded and reprocessing of the transactions are carried out which were logged since the last dump.
→ **Logging changes to the data***:* This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

Operating system controls

Discuss the major tasks performed by Operating System? (**MT- Nov, 14)**
State four major tasks performed by an Operating System while allowing users and their applications to share and access common resources. **(May, 15)**

Major tasks performed by an operating system are given as follow:

- ✓ **Scheduling Jobs:** They can determine the sequence in which jobs are executed, using priorities established.
- ✓ **Managing Hardware and Software Resources:** They can first cause the user's application program to be executed by loading it into primary storage and then cause the various hardware units to perform as specified by the application.
- ✓ **Maintain system Security:** They may require users to enter a password - a group of characters that identifies users as being authorized to have access to the system.
- ✓ **Enabling Multiple User Resources Sharing:** They can handle the scheduling and execution of the application programs for many users at the same time, a feature called multiprogramming.
- ✓ **Handling interrupts:** An interrupt is a technique used by the operating system to temporarily suspend the processing of one program in order to allow another program to be executed. Interrupts are issued when a program requests an operation that does not require the CPU, such as input or output, or when the program exceeds some predetermined time limit.
- ✓ **Maintaining Usage Records:** They can keep track of the amount of time used by each user for each system unit - the CPU, secondary storage, and input and output devices. Such information is usually maintained for the purpose of charging users' departments for their use of the organization's computing resources.

Control objectives: Following are the major control objectives;

- ❖ **Protect itself from user;**
- ❖ **Protect user from each other;**

- **Protect user from themselves;**
- **The OS must be protected from itself; and**
- **The OS must be protected from its environment**.

OS security:

Write short note on Operating System Security **(Nov, 14)**

Describe the various security components available in a Secure Operating system. **(MAY 2006)** (LAAD)

- **L: Log-in procedure:**
- **A: Access Token**
- **A: Access Control List**
- **D: Discretionary Access Control**

Operating System Security: Operating System Security involves **policy, procedure and controls** that determine, 'who can access the operating system', 'which resources they can access', and 'what action they can take'. The following security components are **found in secure operating system**:

- **Log-in Procedure:** A log-in procedure is the **first line of defense** against unauthorized access. When the **user initiates** the log-on process by entering user-id and password, **the system compares the ID and password to a database of valid users.** If the **system finds a match**, then log-on **attempt is authorized**.
- **Access Token:** If the log on attempt is **successful,** the OS **creates an access token** that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is **used to approve all actions attempted** by the user during the session.
- **Access Control List:** This list **contains information** that **defines the access privileges** for all valid users of the resource. When a user **attempts to access a resource**, the system **compasses his or her user-id and privileges contained in the access token** with those contained in the access control list. **If there is a match**, the user is granted access.
- **Discretionary Access Control:** The **system administrator** usually determines; who is **granted access to specific resources** and maintains the access control list. However, resource owners in distributed systems May be granted discretionary access control which allows them to grant access privileges to other users.

Remedy from destructive programs: The following can be used as remedies from destructive programs like viruses, worms etc.:

→ Purchase software from reputed vendor;
→ Examine all software before implementation;
→ Establish educational program for user awareness;
→ Install all new application on a standalone computer and thoroughly test them;
→ Make back up copy of key file; and
→ Always use updated anti-virus software.

System Development Controls

→ **System Authorization Activities:**
→ **User Specification Activities:**
→ **Technical Design Activities:**
→ **Internal Auditor's Participation:**
→ **Program Testing:**
→ **User Test and Acceptance Procedures:**

Computer Centre Security and Controls

These are of the following types: (Papu Singh की Daughter है)

- **Physical Security,**
  - → **Fire Damage:**
  - → **Water Damage:**
  - → **Power Supply Variation:**
  - → **Pollution Damage:**
  - → **Unauthorized Intrusion:**
- **Software & Data Security**, and
- **Data Communication Security**.

Internet and Intranet Controls

Major threats: Component failure and Subversive threats.

Primary component:
Communication Lines:- Hardware: (PMM-SC) Ports, Modems, Multiplexer, switches and concentrator. Software: (Pudina Powder Dangerous hai) Packet switching, pooling software, data compression software etc.
Subversive threats: An intruder attempts to violate the integrity of some components on the sub-system by: Invasive tap and Inductive tap.

(a)Major exposure:

→ **Component Failure:**
→ **Subversive Threats:**
- ✓ **Invasive tap:**
- ✓ **Inductive tap:**
- ✓ **Denial of Service:**

(b) Controls for Subversive Threats: FEC कर Racing Course.

- ❖ **Firewall:**
- ❖ **Encryption:**
- ❖ **Recording of Transaction Log:**
- ❖ **Call Back Devices:**

Personal Computer Control

Mr. 'X' has opened a new departmental store and all the activities are computerized. He uses Personal Computers (PCs) for carrying out the business activities. As an IS auditor, **list the risks related** to the use of PCs in the business of Mr. 'X' and suggest any **two security measures** to be exercised to overcome them. **(Nov, 14)**

1. Risk related to PC

(a) PCs are **small in size & easy** to connect & disconnect, they are likely **to be shifted from** one location to another or even take outside the organisation **for theft of information**.
(b) Pen drive can be **very conveniently transported** from one place to another, as a result of which **data theft may occur**. Even hard disk can be **ported easily** these days.
(c) PC is basically **single user oriented machine** & hence, does **not provide inherent data safeguards**. Problem can be cause by computer **viruses & pirated software**, namely, data corruption, slow operations & system break down etc.
(d) **Segregation** of duties is **not possible**, owing to **limited number of staff**.
(e) Due to **vast number of installations**, the staff **mobility is higher** & hence become **a source of leakage of information**.
(f) The operating staff may **not be adequately trained**.
(g) **Weak access control: Security software** that provides log-on procedures is available for PCs. Most of these programs, however, become active only **when the computer is booted from hard drive**. Disk locks are devices that **prevent unauthorised** individual from accessing the floppy disk or pen drive of a computer.

2. Security measure to overcome risk related to PC.

a. **Physically locking** the system;
b. **Proper logging** of equipment shifting must be done;
c. **Centralise purchase** of hardware & software;
d. **Standards set** for developing, testing and documenting;
e. Uses of **antimalware software**; and
f. **The use** of personal computer & their peripheral must be **controlled**.

Financial Controls:

What do you understand by financial control? Explain major financial controls. **(MT-Nov, 14)**
Explain the various financial control techniques used in information system control. **(May, 14)**

Financial control techniques are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These are numerous; some key techniques are given as follows:
(Just remember 4S BAC DI gS)

- **S: Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **S: Sequentially numbered Documents:** These are working documents with preprinted sequential numbers, which enables the detection of missing documents.
- **S: Supervisory Review:** This refers to review of specific work by a supervisor but what is not obvious is that this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them.
- **Segregation of duties:** This entails assigning similar functions to separate people to provide reasonable assurance against

fraud and provide an accuracy check of the other persons work.

- **B: Budgets:** These estimates the amount of time or money expected to be spent during a particular period of time, project, or event. The budget alone is not an effective control-budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
- **A: Authorisation:** This entails obtaining the authority to perform some act typically access to such assets as accounting or application entries.
- **C: Cancellation of Documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.
- **D: Dual Controls:** This entails having two persons simultaneously access an asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
- **I: Input/ Output Verification:** This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
- **Documentation:** This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.

Organisational Controls

These controls are concerned with the decision making processes that lead to management authorisation of transaction. Organisational controls technique include **documentation of**

- **Reporting responsibility and authority of each function**
- **Definition of responsibilities and objectives of each functions,**
- **Policies and procedures**
- **Job descriptions, and**
- **Segregation of duties.**

Management Controls

The controls adapted by the management of an enterprise are **to ensure** that the information systems function **correctly** and they **meet** the strategic business objectives.The controls considerations while reviewing management controls in an IS system shall include:

→ **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.

→ **An IT Organization Structure:** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.

→ **An IT Steering Committee:** The steering committee shall comprise of representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. Here the responsibility lies beyond just the accounting and financial systems; for example, the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.

BCP (Business Continuity Planning) Controls

These controls are related **to having** an operational and tested IT continuity plan, which is **in line with the** overall business continuity plan, and its **related** business **requirements** so as to make sure IT services are **available as required** and **to ensure a minimum impact** on business in the event of a major disruption.

Example of controls or processes/procedures.

1. Requiring that the contents of a warehouse be periodically counted and reconciled to the inventory recorded on the company's books is a control over the existence and accuracy of inventory.
2. P.C. • **Separating Approval and Payment.** A requirement that an employee who is authorized to initiate a payment to a vendor is not also authorized to sign vendor payment checks would be a preventive control. Among other things, such a control is designed to reduce the risk of unauthorized payments.
3. P.C. • **Limiting Access to IT Systems.** Controlling access to software programs related to accounting or payment functions through the use of passwords and access codes is another type of preventive control. Limiting the persons who can change IT programs reduces the risk of unauthorized transactions.
4. An example of preventive control is the use of password to gain access to a financial system.
5. D.C. • **Reconciliations.** Independently comparing two sets of records that relate to the same transaction and analyzing any differences is a detective control. Reconciling the cash account balance on the company's books to its bank records could identify whether any payments recorded by the company were not received by its bank, or whether any withdrawals reported by the bank were not accounted for by the company.

6. D.C. **Performance Monitoring.** Comparing operating results to budgets or forecasts, or to the results in prior periods, could be a way of highlighting unusual activities. Examining deviations might uncover errors in the records reflecting operating results or unanticipated changes in business activities.
7. Deposit into bank of the entire receipts of a day or daily balancing of the cash book and ledgers or periodic reconciliation with the control accounts are examples of widely used practices which are considered good internal control practices.
8. Audit committee oversight of financial reporting and a CFO's review of differences between the company's monthly budget and actual expenditures are **examples of entity-level controls**.
9. Requiring that delivery receipts be matched with vendor invoices before a vendor payment is authorized is an example of **a process-level control**.
10. Assigning responsibility for physical access to a supply room to a different person than the individual who is responsible for maintaining the records of the supplies inventory is an example of segregation of duties.

The controller who is owner of the general ledger grants only read only privileges to the budgeting department while account payable manager is granted both read as well as write permission to the ledger.

Chapter 4: Business Continuity Planning and Disaster Recovery Planning

संकट/विपदा प्रबंन्धन

आपदा किसे कहते है?

आपदा, एक प्राकृतिक या मानव प्रेरित घटना है जिसके फलस्वरूप व्यापक मानव क्षति **होती** है। इसके साथ–साथ एक निश्चित इलाके मे आजीविका की व संपति की हानि **होती** है जिसके परिणामस्वरूप लोगों को दु:ख एवं कष्ट झेलने पडते हैं।

क्या आपदा को रोका जा सकता है?

आपदा को रोका नहीं जा सकता हैं। आपदा के प्रभाव को कम किया जा सकता है।

खतरा किसे कहते है? (Threat)

हानिकारक परिणामों की संभावना अथवा अपेक्षित हानि ही खतरा है।

संकट किसे कहते है? (Risk)

प्राकृतिक या मानव प्रेरित वह खतरनाक घटना जिससे चोट **लग सकती है,** जीवन नष्ट **हो सकती है** या संपति, आजीविका और पर्यावरण को क्षति **हो सकती है।** संकट कहलाता है।

Needs of Business Continuity Management

What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity. **(Nov, 10) (RTP)**

BCP is **creation and validation** of a practical logistical plan for **how an organisation will recover and restore partially or completely interrupted critical function** within a predetermined time after a disaster or a extended disruption. The logistical plan is called a BCP. Planning is **an activity to be performed before the disaster occurs** otherwise it would be to let to plan an effective response. The **resulting outage from such a disaster can have serious effects** on the validity of a firm's operations, profitability, quality of service, and convenience.

- **Business Resumption Planning**: The **operation peace** of business continuity planning.
- **Disaster Recovery Planning**: The **technological aspect** of BCP, the **advance planning and preparation** necessary to minimise losses and **ensure continuity of critical business functions** of the organisation in the event of disaster.
- **Crisis Management:** The **overall coordination** of organisation **response to a crisis** in effective manner, with the goal of avoiding or minimising damage to the organisation profitability, reputation or ability to operate.

Business Contingency: It is an event with the potential (सम्भावान के साथ) to disrupt computer operations, thereby disrupting critical (महत्वपुर्ण) mission and business function.

BCP Process:

Business Continuity Planning: The ability of enterprise to recover from a disaster and continue operation with the least impact.

OBJECTIVE OF BUSNIESS CONTINUITY

What are the goals and objectives of BCP? **(MT 14N)**

Discuss the objectives and goals of Business Continuity planning.(**Nov, 2008***)*

The **primary objective** of a business continuity planning is to enable an organization **to survive a disaster and to re-establish normal business operations.** In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. The key objectives of the contingency plan should be to:

(i) Provide the **safety and well-being** of people **on the premises** at the time of disaster;
(ii) **Continue** critical business operation;
(iii) **Minimise** the duration of **serious disruption** to operations and resources;
(iv) Minimise **immediate damage and losses**;
(v) Establish management **succession and emergency plan;**
(vi) Facilitate **effective co-ordination** of recovery task;
(vii) **Reduce the complexity** of recovery effort;

(viii) **Identify** critical lines of business and supporting structure. **(RTP 15M)** (**RTP 14N**)

What are the goals of Business Continuity Plan? **(Nov, 12)**

Write short note on Goals of the business continuity plan **(Nov, 13):-** The goals of business continuity plan should be

- **Identify** the weaknesses and implement a disaster prevention program;
- Minimise the duration of serious disruption to operations and resources;
- Facilitate effective co-ordination of recovery task; and
- Reduce the complexity of recovery effort;

Developing a Business Continuity Plan

Methodology Emphasise on the following:

Describe the methodology of developing a Business Continuity Plan. **(Nov. 08)**

Discuss the methodology of developing a Business Continuity Plan. **(May, 14)**

The methodology for developing a business continuity plan can be **sub-divided into eight different phases**. The extent of applicability of each of the phases has **to be tailored to the respective organisation**. The methodology **emphasises** on the following:

1. Providing management with **a comprehensive understanding** of the **total efforts required** to develop and maintain an effective recovery plan;
2. **Obtaining** appropriate **commitment** from top management to support and participate in the effort;
3. **Defining** recovery **requirement** from the perspective of business function;
4. **Documenting** the impact of **extended loss** to operation and key business function;
5. **Focusing** appropriately on disaster **prevention and impact minimisation**, as well as orderly recovery;
6. **Selecting** business continuity teams **that ensure the proper balance** required for plan development;
7. **Developing** a business continuity plan that **is understandable, easy** to use and maintain;
8. **Defining** how business continuity consideration **must be integrated** into ongoing business planning and system development process in order that the plan remains viable over time.

Eight phase for described:

Name the different phases of methodology for developing a BCP. What are the major points on which a methodology emphasises upon? **(MT 14)** (**P**rabhu **V**ishnu के घर पर **B**aby **D**oll **P**erform करती है **TMI** show)

(i) Pre-planning activities,
(ii) Vulnerability Assessment and General Definition of requirement, (RTP 14N)
(iii) Business Impact Analysis,
(iv) Detailed Definition of Requirement,
(v) Plan Development,
(vi) Testing Program,
(vii) Maintenance Program, and
(viii) **Initial Plan Testing and Plan Implementation. (RTP 15M)**

Maintenance Task undertaken in development of BCP (**RTP 14N**)

Explain the objectives of Business Continuity Management Policy briefly. **(Nov, 14)**

The objective of Business Continuity Management Policy is **to provide a structure through which**:

→ **The loss to** enterprise's business **in terms of** revenue loss, loss of reputation, loss of productivity and customer satisfaction **is minimized.**
→ **Critical** services and activities undertaken by the enterprise operation for the customer will be **identified.**
→ **Plans** will be **developed** to ensure **continuity** of key service delivery following a business
→ **Disruption**, which may arise from the loss of facilities, personnel, IT and/or communication or failure within the supply and support chains.
→ **Invocation** of incident management and business continuity plans can be managed.
→ **Incident** Management Plans & Business Continuity Plans are **subject to ongoing testing, revision and updation** as required.
→ Planning and management responsibility are **assigned to a member of the relevant senior** management team.

What are the tasks you will undertake to ensure that BCM program is in place, while assessing **BIA**? **(May, 15)**

Business Impact Analysis (BIA) is essentially a means **of systematically assessing** the potential impacts resulting from various events or incidents. The tasks to be undertaken to ensure that BCM program is in place while assessing BIA are as follows:

- **Assess the impacts** that would occur if the activity was disrupted over a period of time;
- **Identify the maximum time period** after the start of a disruption within which the activity needs to be resumed;
- **Identify critical** business processes;

- **Assess the minimum level at** which the activity needs to be performed on its resumption;
- **Identify the length of time** within which normal levels of operation need to be resumed; and
- Identify any **inter-dependent activities**, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

Types of Plans (Just remember **RET-B**)

Difference between backup and recovery plan**. (MT 15M)**
Explain the various general components of Disaster Recovery Plan.' **(Nov, 11)**
Out of various types of plans used in business continuity planning, discuss recovery plan in brief. **(May, 12)**
Explain the various plans that need to be designed for business continuity management**. (Nov, 15)**
What do you understand by disaster recovery plan? Discuss its various components. (**MAY 2005)**

Disaster Recovery Plan – The term disaster recovery **describes the contingency measures** that organizations **have adopted at key computing sites to recover from** or to prevent any monumentally bad event or disaster. A disaster may **result from natural causes** such as fire, flood or earthquake etc. or **from other sources** such as a violent takeover, willful or accidental destruction of equipment or any other act of such catastrophic proportion that the organization could be ruined. The **primary objective** of a disaster recovery plan is **to assure the managemen**t that **normalcy would be restored** in a set time after any disaster occurs, **thereby minimizing losses** to the organization.

Although each organization would **have its own tailored** disaster recovery plan, **the general components** of the plan are as follows:

(1) Emergency Plan – It **outlines** the actions to be undertaken **immediately after** a disaster occurs. It **identifies** the personnel to be notified immediately. It **provides guidelines** on shutting down equipment, termination of power supply, removal of storage files, and removable discs. It **sets out evacuation procedures**. It also provides **return procedures** as soon as the primary facility is ready for operation like backing up data files at off-site, deleting data from disk drives at third party site, relocation of proper versions of backup files etc.

(2) Recovery Plan – This part of disaster recovery plan **sets out** how the **full capabilities will be restored**. The following steps may be carried out under this plan: **(RTP)**

(i) Inventory of hardware, application systems, system software, documentation etc. must be taken.

(ii) Criticality of application systems to the organization and the importance of their loss must be **evaluated**. **An indication** must be given **of the efforts and cost involved** in restoring the various application systems.

(iii) An application systems **hierarchy** must be **spelt out.** This would be **used** when the management **decides to accept** a **degraded mode of operation**.

(iv) Selection of a disaster recovery **site** must be made. A **reciprocal agreement** with another organization **having compatible hardware and software could be made**.

(v) Formal backup arrangement should be made. This should cover the **periodical exchange of information** between the two sites regarding changes to hardware / software, the time and duration of system availability.

(3) Backup Plan – Organization no matter how physically secure, their systems are **always vulnerable to the disaster**. Therefore, an effective safeguard is **to have a backup of anything** that could be destroyed, be it hardware or software. As far as software is concerned, it is necessary to **make copies of important programs**, data files, operating system and test programs etc. **in order to get back into operation** before the company can suffer an intolerable loss. Often, the originals are stored **at a site that is physically distant** from the actual site and where duplicate copies are used for processing. The backup copies must be kept in a place, which is **not susceptible to the same hazards** as the originals.

(4) Test Plan – Test Plan looks after the testing of DRP and analysis of the result. It **identifies deficiencies** in the emergency, backup or recovery plan. It contains procedures for conducting DRP testing like:

(i) **Paper Walkthrough** - It involves critical personnel in the plan's execution, reasoning out what might happen in the event of different disasters.

(ii) **Localized Tests** - It simulates system crash. This test is performed on different aspects of DRP.

(iii) **Full operational test** - It is nearer to disaster conditions. Paper walkthrough and localized test should have been conducted before completely shutting down the operation to simulate disasters.

Types of Back-ups

Briefly explain the various types of system's back-up for the system and data together. **(Nov. 08)**

Write short note on types of Back up **(Nov, 14)** Discuss various types of back-up plans used in BCP**? (MT 14N)** What are various backup techniques? Which backup technique, you will recommend and why ? **(Nov,11)**

Types of system's Back-ups: When the back-ups are taken of the system and data together, they are called Total System's Back-up. Various types of back-ups are given as follows: **(FuIn DiMi)**

→ **Full backup**: It captures all files on the disk or within folder selected for backup. Every backup generation contains every file in the backup set. **(RTP-15M). (RTP 14N)**

→ **Incremental Backup:** It captures files that were created or changed since last backup, पिछला backup का type कोई भी हो सकता है. **(RTP-15M).**

→ **Differential Backup**: It stores/captures files that have changed since last full backup. पिछला full backups रहता है. **(RTP 14N)**

→ **Mirror Backup**: It is identical to full backup, with the exception that files are not compressed in zip files and they cannot be protected with the password.

Alternate Processing Facility Arrangement (Backup options)

Discuss the various backup options considered by a security administrator when arranging alternate processing facility. **(May, 11)) (May, 15)** (**CoHoWaR**

Security administrators should consider the **following backup options** while arranging alternate processing facility:

→ **Cold site**: If orgⁿ can **tolerate some downtime**, this backup **might be appropriate**. A cold site **has all the facilities** needed to install a mainframe system, raised floors, air conditioning, power, communication lines, and so on. An organization can **establish its own cold site facility or enter into an agreement with a**nother organization to provide a cold site facility.

→ **Hot Site**: If **fast recovery** is critical, an organization **might need hot site backup**. All hardware and operations facilities will be available at the host site. In some cases, software, data and supplies might **also be stored there**. A hot site is **expensive to maintain**. They are **usually shared** with other organizations that have hot site needs.

→ **Warm site:** It provides an **intermediate level of backup**. It has all cold site facilities in addition with hardware that might be difficult to obtain or install. For example, a warm site might **contain selected peripheral** equipment plus a small mainframe with sufficient power to handle critical applications in the short run.

→ **Reciprocal Agreement:**

A company has decided to outsource a third party site for its alternate back-up and recovery process. What are the issues to be considered by the security administrator while drafting the contract? **(May, 10)**

Two Two or more organizations **might agree to provide backup facilities to each other** in the event of one suffering a disaster. This backup option is relatively cheap, but each participant **must maintain sufficient capacity to operate another's critical system**.

Issue to be covered in reciprocal agreement;

- **How soon** the site will be made available subsequent to the disaster;
- The **number of the organisation** that will be allowed to use the site concurrently in the event of disaster;
- The **priority to be given** to concurrent users of the site in the event of a common disaster;
- The **period** during which the site can be used;
- The **conditions** under which site can be used;
- The **facilities and services** that the site provider agrees to make available; and
- **What control** will be in the place and working at offsite facility. (**RTP 14N**)

What factors should be verified while auditing or self assessment of the enterprise's BCM program? **(RTP 15M)**

While doing audit or self assessment of the BCM Program of an enterprise, briefly describe the matters to be verified. **(Nov, 14)**

As an IS auditor, what are the key **areas you would verify** during review of BCM arrangements of an enterprise.**(May, 15)**

An audit or self-assessment of the enterprise's BCM (Business Continuity Management) program should verify that:

During review of BCM arrangements of an enterprise, an IS auditor should verify that:

→ **All key** products and services and their supporting critical activities and resources have been **identified and included** in the enterprise's BCM strategy;

→ The enterprise's BCM policy, strategies, framework and plans **accurately reflect its priorities and requirements**;

→ The enterprise' BCM competence and its BCM capability are **effective and fit-for-purpose** and will **permit management, command, control and coordination** of an incident;

→ The enterprise's BCM solutions are **effective, up-to-date and fit-for-purpose, and appropriate** to the level of risk faced by the enterprise;

→ The enterprise's BCM **maintenance and exercising programs** have been **effectively implemented**;

→ BCM strategies and plans **incorporate improvements identified** during incidents and exercises and in the maintenance

program;
→ The enterprise has **an ongoing program** for BCM training and awareness;
→ BCM **procedures** have been **effectively communicated** to relevant staff, and that those staff understand their roles and responsibilities; and
→ **Change control processes** are **in place and operate effectively**.

What do you understand by the term "Risk Assessment" in term of Network Security?
Solution: Simply reproduced matter of chapter 4 para 4.8.3.

What do you understand by the term Disaster? What procedural plan do you suggest for disaster recovery? **(Nov, 08)**
The term disaster can be defined as **an incident which jeopardizes business operations** and/or human life. It could be due to sabotage (human) or natural. Following is the procedural plans for disaster recovery.

Disaster Recovery Procedural Plan: Normally disaster recovery procedural **plan is made when the system is normally working**. **After visualizing the disaster the action to be taken** by different people of the organization are **to be documented**. This recovery and planning document may **include the following areas**:

- **The conditions for activating the plans**, which describe the process to be followed before each plan, is activated.
- **Emergency procedures,** which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning with appropriate public authorities e.g. police, fire, services and local government.
- **Fallback procedures**, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
- **Resumption procedures,** which describe the actions to be taken to return to normal business operations.
- **A maintenance schedule**, which specifies the process for maintaining the plan.
- Awareness and education activities, which are **designed to create an understanding** of the disaster recovery process.
- **The responsibilities** of individuals describing who is responsible for **executing which component** of the plan. **Alternatives should be nominated as required.**
- **Contingency plan** document distribution list.
- **Detailed description** of the purpose and scope of the plan.
- **Contingency plan** testing and recovery procedure.
- **List of vendors** doing business with the organization, their contact numbers and address for emergency purposes.
- **Checklist for** inventory taking and updating the contingency plan on a regular basis.
- **List of phone numbers** of employees in the event of an emergency.
- **Emergency phone list** for fire, police, hardware, software, suppliers, customers, back-up location, etc.
- **Medical procedure** to be followed in case of injury.
- **Back-up location** contractual agreement, correspondences. Insurance papers and claim forms.
- **Primary** computer center hardware, software, peripheral equipment and software configuration.
- **Location of** data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
- **Alternate** manual procedures **to be followed** during the period of disruption such as manual preparation of invoices.
- **Names** of employees **trained for emergency** situation, first aid and life saving techniques.
- **Details** of airlines, hotels, supplies and transport arrangements.

How an auditor will determine whether the disaster recovery plan was developed using **a sound and robust methodology**? Explain. **(Nov, 13)**

OR

What are the **elements to be included** in the methodology for the development of disaster recovery / business resumption plan? **(Nov, 12)**
The elements to be included in the methodology for the development of a disaster recovery/business resumption plan are given as follows:

- **Identification and prioritization** of the activities, which are essential for continuous functioning.
- Determining that the plan **is based upon a business impact analysis**, which considers the impact of the loss of essential functions.
- Determining that Operation managers and key employees **participated in the development of the plan**.
- Determining that the plan **identifies the resources** that will likely to be needed for recovery and the location of their

availability.

- ❖ Determining that the plan is **simple and easily understood** so that it will be effective when it is needed.
- ❖ Determining that the plan is **realistic in its assumptions**.

While auditing a Disaster' Recovery Plan (DRP) for information technology (IT) assets, **what concerns are required to be addressed**? Briefly explain. (**May, 14**)

While auditing a Disaster Recovery Plan (DRP) for IT assets, the following concerns are required to be addressed:

- ✓ Determine if the plan **reflects the current IT environment**.
- ✓ Determine if the plan **includes prioritization of critical applications and systems**.
- ✓ Determine if the plan includes **time requirements** for recovery/availability of each critical system, and that they are reasonable.
- ✓ Does the disaster recovery/ business resumption plan **include arrangements for emergency telecommunications**?
- ✓ Is there a plan **for alternate means of data transmission** if the computer network is interrupted? Has the security of alternate methods been considered?
- ✓ Determine if a **testing schedule exists** and is adequate (at least annually).
- ✓ Verify the **date of the last test**. Determine if **weaknesses identified** in the last tests were corrected.
- ✓ Determine if information **backup procedures are sufficient** to allow for recovery of critical data.
- ✓ Determine **if copies of the plan are safeguarded** by off-site storage.
- ✓ Does the disaster recovery/ business resumption plan **include provisions for Personnel**?

Chapter 5: Acquisition, Development and Implementation of Information System

System Development:

In business, system development refers to the process of examining **a business situation** in the prevailing context with the intent of improving it through **better procedures and methods**.

The process of system development **starts** when management or sometimes system development personnel realise that a particular business system needs improvement (SDLC कब start होता है).

The System development process is initiated when it is realised that a particular business process of the organisation need computerisation or improvement.

The business process: The unique way in which enterprise coordinate and organise work activities, information, and knowledge to produce product or service.

Business Process Design:

It means structuring or restructuring the tasks, functionalities and activities for improving a business system. यह जरूरी है to understand requirement of the system.

Failure to achieve the objective of a system development (RTP 14N), (QPM) (MT May, 15)

Bring out the reasons as to why the organizations fail to achieve their Systems Development Objectives? **(May, 03)**

Many-a-time organizations fail to achieve their system development objectives. Justify the statement giving reasons. **(May, 15**

Reason due to which organisation fail to achieve their system development objective are;

(a)User related issues **(RTP 15M) (SLR-India)**

- → **Shifting user needs:** Users requirements for IT system are constantly changing. More request for IS and more development project.
- → **Resistance to change:** Natural tendency to resist change, and IS development project signal changes in the work place. Dig in their hills, & project is doomed to failure.
- → **Lack of user participation:** Not participate in development project because preoccupied with existing work.
- → **Inadequate testing & training:** Often system is not tested due to lack of time & rush to introduce new system. Result failure to test.

(b) Developer related issues

- → **Methodologies: Non-formalisation of project management and system development Methodologies.**
- → **Overworked or under trained development staff: Lack of sufficient educational background and requisite states of skills.**

(c)Management related issues.

- → **Lack of senior management support and involvement:** watch senior management to determine 'which system development projects are important'.
- → **Development of strategic system: Decision makings are unstructured.**

(d)New technology: Attaining system development objective is more difficult because personnel are not familiar with the technology.

System Development Methodology:

It is a **formalised, standardised, well-organized and documented** set of activities used to manage a system development project. (Project manage कैसे करना है)

The methodology is characterised by the following:

- The project is divided into number of identifiable process (project को विभाजीत करें) and each phase has starting point and an ending point. Each process comprises several activities, one or more deliverables and several management control points. Project का विभाजन small and manageable size मे करने से मदद मिलता है planning and project control मे.
- समय-समय पर specific report produce करना बहुत जरूरी है system develop करते समय to make development team accountable for faithful execution of system development task.
- Users, managers and auditor are required to participate in the project, वे समान्यत: मंजुरी देतें है पुर्वनिंधरित management control point पर. Sign off signify approval of development process.
- The system must be tested prior to implementation to ensure that it meets user needs as well as requisite functionality.
- A training plan is developed who will operate and use the new system.
- Formal program change controls are established to prevent unauthorised changes to computer programs.
- A post implementation review must be performed to assess the effectiveness and efficiency of the new system and of the development process.

System Development Methodologies.

All these approaches are not mutually exclusive, which means that it is possible to perform some prototyping while applying waterfall approach. ऐ सभी approaches एक के बाद एक अस्तित्व मे आऐ हैं इस से साफ जाहिर है हर अगला approach पिछले approach का weakness को दुर करने कि एक प्रयास है.

Waterfall Model

Describe the strength, of waterfall approach to system development. **(May, 14)**

इसमे प्रतेयक phases are carried out in sequence. Phases are all the phases of SDLC. यहाँ एक activity/phase शुरू किया जाता है only when the prior step is fully completed. Strength & weakness **(RTP 15M)**

Major strengths of waterfall approach are given as follows:

- This model is ideal for supporting less experienced project teams and project managers or project teams whose composition fluctuates.
- An orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software.
- Progress of system development is measurable in this model. It conserves resources also.

The Prototyping Model

As a person in-charge of System Development Life Cycle, you are assigned a job of developing a model for a new system, which combines the features of a prototyping model and the waterfall model. Which will be the model of your choice and what are its strengths and weaknesses? **(Nov, 10)**

As a person in-charge of system development life cycle, the spiral model will be the choice. The spiral model is a software development process, combining elements of both design and prototyping-in-stages, in an effort to combine/ advantages of top-down and bottom-up concepts. It is a system development method, which combines the features of the prototyping model and the waterfall model.

What is the goal of a prototype model approach of software development? Enumerate the strength of this model**. (May, 13)**

What is prototyping approaches to systems development? Describe its **advantages and disadvantages** also. **(MAY, 07)**

It used in developing non recurring systems. PROTOTYPE is a system with basic functionality. A prototype एक usable system or system component है जो तुरन्त (यानी की कम समय मे) और कम लागत मे तैयार हो जाता है, और modify/replace/expand करने के इरादे के साथ or even replacing it by a full-scale and fully operational system. Waterfall model मे एक system develop करने मे कई वर्ष लग जाता थे। Prototyping Model केवल product जो market के लिए नया है ऊसके लिए use किया जाता है। Competitive market मे नहीं use करना चाहिए। Strength **(RTP 14N)**

Prototyping technique is used to develop **smaller systems** such as decision support systems, management information systems and expert systems. **The goal** of prototyping approach is **to develop a small or pilot version** called a prototype of part or all of a system. A prototype is a **usable system or system component** that is built quickly **and at a lesser cost**, and with **the intention of being modifying** or replacing it by a full scale and fully operational system. **Finally**, when a prototype is developed that satisfies all user requirements, either **it is refined and turned** into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is develop the real system.

जब users prototype के साथ काम करते है तब वेलोग learn करते हैं about the system criticalities and make suggestions about the way to manage it. These suggestions are then incorporated to improve the prototype, such improved prototype is also used and evaluated. अन्त मे, जब एक prototype develop किया जाता है जो satisfies करताा है all user requirement, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Discuss the four steps of the prototyping approach in system development. **(May, 04)**

The generic phases of this model are explained as follow

- **Identify information system requirement:** In traditional approach, the system **requirements** have **to be identified before** the development process starts. However, under prototype approach, the design team **needs only fundamental system requirements** to build the initial prototype, the process of determining them can be **less formal and time-consuming** than when performing traditional systems analysis. The team can develop the **detailed requirements** of the system **later after** users have had time to interact with the prototype and provide feedback.
- **Develop Initial Prototype**: In this step, the designers **create an initial base model** – for example, using fourth-generation programming languages or CASE tools. In this phase, **the goals** are **"rapid development" and "low cost**." Thus, the designers give little or no consideration to internal controls, but instead emphasize on such system characteristics as **"simplicity," "flexibility," and "ease of use."** These characteristics enable users **to interact with tentative versions** of data entry display screens, menus, input prompts, and source documents. The users also need to **be able to respond** to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.
- **Test and revise**: After finishing the initial prototype, the designers **first demonstrate** the model to users and **then give** it to them to experiment. **At the outset**, users must be told that the prototype is incomplete and requires subsequent modifications based on their feedback. Thus, the **designers ask users to record their likes and dislikes about** the system and recommend changes. Using this feedback, the design team **modifies the prototype as necessary** and **then resubmits** the revised model to system users for revaluation. Thus, iterative process of modification and revaluation continues until the users are satisfied – commonly, through four to six interactions.
- **Obtain User Signoff of the approved prototype:** At the end of Step 3, users **formally approve the final version** of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide. Approximately **half of these** approved prototypes become **fully functional systems**. **The remaining**, throwaway prototypes are not developed – typically because the modifications required to make them functional are too costly or in other ways not practical. But this does not mean that the prototyping exercise has been a failure. To the contrary, it signals an impractical system and thus saves an organization a great deal of time and money.

Advantages of Prototyping

1. Prototyping requires **intensive involvement** by the system users. Therefore, it typically results in **a better definition** of the users' needs and requirements than does the traditional system development approach.
2. A **very short time period** (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
3. Since system users experiment with each version of the prototype through an interactive process, **errors are hopefully detected and eliminated** early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

Disadvantages of Prototyping

1. Prototyping can only be successful if the system users are **willing to devote significant time in experimenting** with the prototype and provide the system developers with change suggestions.
2. The interactive process of prototyping **causes the prototype to be experimented with quite extensively**. Because of this, the system developers are **frequently tempted to minimize the testing** and documentation process of the ultimately approved information system. Inadequate testing can make the approved system error-prone, and inadequate documentation make this system difficult to maintain.
3. Prototyping may cause **behavioral problems** with system users. These problems include **dissatisfaction by users** if system developers are **unable to meet all user demands for improvements** as well as dissatisfaction and impatience by user when they have to go through too many interactions of the prototype.

Strengths:

(i) Enhance risk avoidance;

(ii) Useful in helping to select the best methodology to follow for development of a given software iteration based on project

risk. Can incorporate waterfall, prototyping and incremental methodologies as special cases in the framework, and provide guidance as to which combinations of these models best fits a given software iteration, based upon the type of project risk.

Weaknesses:

(i) Challenges to determine the **exact composition of development methodologies** to use for each iteration around the spiral.

(ii) **Highly customized** to each project and thus is quite complex, limiting reusability.

(iii) A skilled and experienced project manager **required** to determine how to apply it to any given project.

(iv) **No established controls** for moving from one cycle to another cycle. Without controls, each cycle may generate, more work for the next cycle.

(v) **No firm deadlines** cycles continue **with no clean termination condition**, so there is an inherent risk of not meeting budget or schedule.

The incremental Model

यहाँ product को design, implement and test किया जाता है incrementally जब तक product finish ना हो जाए। incremental design, implementation and test करने के लिए product को decompose करना पडता है into number of components. Each component is delivered to client when it is complete.

Spiral Model

It combines elements of both design and prototyping **in-stages**.
It tries to combine advantage top-down and bottom up **concepts**.
It combines the **features** of prototyping model and waterfall model.
Spiral model is used in game development.

RAD Model

It is used to develop complex systems rapidly or in lesser time. It uses **minimal** planning in favour of rapid prototyping. Planning is interleaved with writing software itself. Lack of pre-planning **allows** software to be written in much faster, and **makes it easier to change requirements.**

Agile Model

Strength & weakness **(MT, 15M)**

Describe the Agile Methodology of system development. Describe its strength. **(Nov, 13)**

Define the AM of software development & discuss its strengths**. (Nov, 14) RTP**

This is a **group of software** development methodologies based on the ***iterative and incremental*** **development**, where requirements and solutions **evolve through collaboration** between self-organizing, cross-functional teams.

It **promotes** adaptive planning, evolutionary development and delivery; time boxed iterative approach and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen interactions throughout the development life cycle.

Major strengths of agile methodology are given as follows:

- Agile methodology has the **concept of an adaptive** team, which is able to respond to the changing requirements.
- The team does **not have to invest time and efforts** and finally find that by the time they delivered the product, the requirements of the customer have changed.
- Face-to-face communication and continuous inputs from customer representative **leaves no space for guesswork**.
- The documentation is crisp and to-the-point to save time.
- The end result is the **high quality software** in least possible time duration and satisfied customer.

System Development Life Cycle

Discuss the various activities which are part of the system development life cycle. (**NOV, 07)**

just we have to write all the phases of SDLC

Overview:

A SDLC is **composed** of a number of **Clearly Defined and Distinct Work Phases** which are used by system engineer and system developer **to Plan for, Design, Build, Test, and Deliver** Information System.

Like anything which is manufactured on an assembly line, an SDLC aims to produce high quality system that meet or exceed customer expectations, based on customer requirements, by delivering system which move through each clearly defined phase within schedule time-frame and cost estimates.

Computer systems are complex and often link multiple traditional systems potentially supplied by different software vendors. To manage this level of complexity, a number of SDLC models have been created, such as:

- Waterfall Model
- Prototyping Model
- Incremental Model
- Spiral Model
- Agile Model
- Rapid Model

Need of Emergence of Different Methodologies: The Traditional life cycle approaches to system developments have been increasingly **replaced with alternative approaches and framework** which attempt to overcome some of the inherent deficiencies of the traditional SDLC.

Some of the phase elaborated for General Knowledge

Preliminary Investigation:–

- Conduct the preliminary investigation: In this step you need to find out the organisation's objectives, and nature & scope of the problem under study. Even if a problem refers only to a small segment of the organisation itself then you need to find out what the objectives of the organisation itself are. Then you need to see how the problem being studied fits in them.
- Propose alternative solution:- In digging into organisation's objective and specific problems, you may have already covered some solution. Alternative proposal may come from interviewing clients, suppliers, and/or consultants. You can also study what competitors are doing. With this data, you will have three chices:
  - Leave the system as is,
  - Improve it, or
  - Develop a new system.

❖ Describe the Costs and Benefit:

System Requirement Analysis:–

Define project goals into defined functions and operations of intended application. It is the process of gathering and interpreting facts, diagnosing problems and recommending improvement to the system. Analyses end-user requirements and also removes any inconsistencies and incompleteness in the requirements.

Steps;

- Collection of facts:-
- Scrutiny of the existing system:- identifying pros and cons of existing system in place, so as to carry forward the pros and avoid the cons in the new system.
- Analysis of proposed system:- Solution to shortcoming in step2 are found and any specific user proposals are used to prepare the specification.

What is a system development Life-cycle? **(May, 04)**

Write short notes on System Development Life-cycle. **(Nov, 04)**

SDLC is the set of activities that a system analyst has to carry out to develop and implement an IS under various approaches of development. It consist of mainly six activities: In most business situations, these activities are all closely related usually in-separable and even the order of the steps in these activities may be difficult to determine.

It provides system designer and developer **to follow a sequence** of activities (i.e. steps).

It is document driven (it means प्रतेयक step complete होने पर document produce किया जाता है और एक phase तब तक complete नहीं होगा जब तक document produce नहीं किया जाता है). Documentation जरूरी है for successful management of the project.

Advantages of SDLC are

❖ Better planning and control by project manager;

❖ **Compliance** to prescribed standards **ensure better quality;** (SDLC मे system develop & design करने के standards दिए होते हैं)

❖ **Documentation** is an important measure of communication and control; and

❖ The phases are important milestone help the project manager and the user for review and signoff.

What are the possible advantage of SDLC from the prospective of IS audit? **(PM)**

IS audit के दृष्टिकोण से following advantages है

From the perspective of IS audit, what are the advantages of System Development Life Cycle? **(Nov, 10)**

State the advantages of SDLC from the perspective of the IS Audit. **(Nov, 12)**

➢ The IS Auditor can have clear understanding of various phases on the basis of documentation created during the each phase of the SDLC.

- The IS auditor on the basis of his **examination**, can state in his **report** about the compliance by the IS management of the procedures, if any, set by the management.
- The IS auditor can be **a guide** during the various phase of SDLC, if he has technical knowledge and ability of different areas of SDLC.
- The IS auditor can provide **an evolution** of the methods and techniques used through the various development phases of the SDLC.

Shortcoming of SDLC:

Cumbersome, end product is not visible for a long time, prolong duration of many project, not suitable for small and minimum sized project.

Discuss the various activities which are part of the system development life cycle. ***(5 Marks, November 2007)***
State and briefly explain six stages of System Development Life Cycle (SDLC). ***(10 Marks, November 2008)***

System Development Life Cycle: The system development process is initiated when it is realized that a particular business process of the organization needs computerization or improvement. The system development life cycle is a set of six activities which are closely related. These activities after a certain stage can be done parallel to each other. For example the development can be started for some components (sub-systems) which are at the advanced stage of designing. The systems development life cycle method consists of the following activities:

- Preliminary investigation,
- Requirements analysis or systems analysis,
- Design of system,
- Development of software, Systems testing, and
- Implementation and maintenance.

The activities are briefly explained below:

Preliminary investigation: When the 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. It consists of **three parts**; Request Classification Feasibility Study and Request Approval. Generally the request submitted is not stated clearly: hence requires detailed study. On receipt of request and identification of needs, the feasibility study is conducted which includes the aspects related to technical, economic and operational feasibility and is normally conducted by a third party depending upon the quantum and size of the requirements. Approval is sought from top management to initiate the system development.

Requirements analysis or systems analysis: Once the request of the system development is approved, the detailed requirement study is conducted in close interaction with the concerned employees and managers to understand the detailed functioning, short-comings, bottlenecks and to determine the features to be included in the system catering to the needs and requirements of users. This process is termed as "System Requirement Study (SRS)" or System analysis.

Design of the system: This activity evolves the methodology and steps to be included in the system to meet identified needs and requirements of the system. The analyst designs the various procedures, report, inputs, files and database structures and prepares the comprehensive system design. These specifications are then passed on to the Development Team for program coding and testing.

Acquisition and development of software: Once the system design details are resolved and SRS is accepted by the user, the hardware and software details along with services requirements are determined and procured choosing the best-fit options. Subsequently, choices are made regarding which products to buy or lease from which vendors. The choice depends on many factors such as time, cost and availability of programmers. In case of in-house development, the analyst works closely with the programmers. The analyst also works with users to develop documentation for software and various procedure manuals.

Systems testing: Once all the programs comprising the system have been developed and tested, the system needs to be tested as a whole. System testing is conducted with various probable options and conditions to ensure that it does not fail in any condition. The system is expected to run as per the specifications made in the SRS and users' expectations. Live test data are input for processing, and results are examined. If it is found satisfactory, it is eventually tested with actual data from the current system.

Implementation and maintenance: By the time of accomplishment of the above activities, it is ensured that the requisite hardware and software are installed and the users are trained on the new system to carry out operations independently. For sometimes, hand-holding may be done by the system development team. The operations are monitored closely to ensure users' satisfaction. The system is maintained and modified to adapt to changing needs of users and business to ensure long-term acceptance of the system.

Phase Description

Phase I: Preliminary Investigation

(Diagnosis stage i.e. identify which illness or problem a person is suffering from by examine the symptom) इस phase का ऊद्धेश्य निर्धारित करना और विश्लेषण करना है **strategic benefit** in implementing system **through** evaluation and quantification of –

→ Productivity gain;
→ Future cost avoidance;
→ Cost saving; and

→ Intangible Benefit.

Requirement engineer will tackle the issues and feasibility study (ऊपयोगीता अध्यन) for the following;

- निर्धारित करना whether the solution is as per the business strategy;
- निर्धारित करना whether the existing system can rectify the situation without a major modification;
- निर्धारित करना the approximate cost to develop the system;
- निर्धारित करना whether the vendor product offers a solution to the problem; and
- Define the time frame for which solution is required.

Steps in PI

Step 1: Identification of problem: User request for new system or change in existing system is properly defined by analysts. Define problem clearly & precisely (सक्षिप्त), जो किया जाता है केवल after the critical study of वर्तमान system और several round of discussion with the user group. Then problem prevalence organisation मे has to be assessed. जिस problem का व्यापक प्रभाव organisation मे होता है is likely to receive immediate management attention.

Step 2: Identification of objective (किसका objective): **After identification of the problem**, it is easy to work out and precisely **specify the objective** of the proposed solution.

Step 3: Delineation of Scope (किसका Scope): The scope of a solution **defines its typical boundary**. Scope clear and comprehensible होना चहिए to user management. Scope state करेगा "what will be addressed by the solution and what will not". प्राय: Scope विवाद का मसला बन जाता है between development and user organisation. इसलिए scope प्रारम्भ मे explain कर देना चहिए। The typical **scope determination may be performed** on the following dimension; functionality requirement, data to be processed, performance requirement, constraint, interface, reliability requirement.

What are the Two Primary Methods through which the analyst would have collected date? **(RTP 14N)**
Explain Two Primary Methods, which are used for the analysis of the scope of a project in SDLC.
What are the two primary methods through which the analyst would have collected the data. **(May, 10)**

These are:

- **Reviewing Internal Documents:** The analysts try to learn about the orgⁿ involved in or affected by, the project.
- **Conducting Interview:** Interview allow analysts to know more about the nature of the project request and the reason for submitting it.

Step 4: Feasibility Study. **(MT Nov, 14)**

The top management of company has decided to develop a computer information system for its operations. Is it essential to conduct the feasibility study of system before implementing it? If answer is yes, state the reasons. Also discuss three different angles through which the feasibility study of the system is to be conducted. **(May, 09)**

Yes, it is essential to carry out the feasibility study of the project before its implementation. After possible solution options are identified, project feasibility-the likelihood that these systems will be useful for the organization-is determined. Feasibility study refers to a process of evaluating alternative systems through various angles so that the most feasible and desirable system can be selected for development. It is carried out by system analysts.

The Feasibility Study of the system is **undertaken from three angles** i.e. Technical, Economic and Operational. The proposed system is evaluated from a technical view point first and **if technically feasible**, its impact on the organization and staff is assessed. If a compatible technical and social system can be devised, it is then tested for economic feasibility.

Project Feasibility - i.e. "संभावनाऐं कि ये systems **ऊपयोगी** होगें organisation के लिए" – is determined (तय किया जाता है।).

Project Feasibility is a test (जाँच/परीक्षण) by which an investment is evaluated. System analyst के द्वारा किया जाता है। Feasibility (ऊपयोगीता) study of a system is evaluated **under following dimensions**;

- ✓ **Technical**: क्या आवश्यक technology available है?
- ✓ **Financial**: क्या the solution viable financially है?
- ✓ **Economic**: ROI?
- ✓ **Schedule/time**: क्या system समय पर deliver किया जा सकता है? **(RTP-15M).**
- ✓ **Resources**: क्या human resource को solution मे अरूची है?
- ✓ **Operational**: Solution कैसे work करेगा?
- ✓ **Behavioral**: is the solution going to bring any adverse effect on quality of work life?

✓ **Legal**: is the solution viable in legal terms?

Technical Feasibility: It is concerned with hardware and software. Essentially, the analyst ascertains whether the proposed system is feasible with existing or expected computer hardware and software technology. The technical issues usually raised during the feasibility stage of investigation include the following:

- Does the necessary **technology exist** to do what is suggested (and can it be acquired)?
- Does the proposed equipment have the **technical capacity** to hold the data required to run the new system?
- Will the proposed system provide **an adequate response** to inquiries, regardless of the number or location of users?
- Can the system be **expanded if developed**?
- Are there **technical guarantees** of accuracy, reliability, ease of access, and data security?

Economic Feasibility: It includes an evaluation of **all the incremental costs and benefits expected** if the proposed system is implemented. This is the most difficult aspect of the study. The financial and economic questions raised by analysts during the preliminary investigation are for the purpose of estimating the following:

- The cost of conducting a full system investigation.
- The cost of hardware and software for the class of applications being considered. The benefits in the form of reduced costs or fewer costly errors.
- The cost if nothing changes (i.e. the proposed system is not developed).
- The procedure employed is the traditional cost-benefit study.

Operational Feasibility: It is concerned with ascertaining the **views of workers**, employees, customers and suppliers about the use of computer facility. The support or lack of support that the firm's employees are likely to give to the system is a critical aspect of feasibility. A system can be **highly feasible** in all respects except the operational and fails miserably **because of human problems**. Some of the questions, which may help in conducting the operational feasibility of a project, are stated below:

- Is there **sufficient support** for the system from management and from users? If the current system is well liked and used to the extent that persons will not be able to see reasons for a change, there may be resistance.
- Are current **business methods acceptable to user**? If they are not, users may welcome a change that will bring about a more operational and useful system.
- Have the users been **involved in planning and development** of the project? Early involvement reduces chances of resistance to the system and changes in general and increases the likelihood of successful projects.
- Will the proposed system **cause harm**? Will it produce poorer results in any respect or area? Will loss of control result in any area? Will accessibility of information be lost? Will individual performance be poorer after implementation than before? Will performance be affected in an undesirable way? Will the system slow performance in any area?

Reporting result to management;

Internal control Aspects

The analyst working on the PI **should** accomplish the following objectives (**करना चहिए);**

- Clarify and understand the project request;
- निर्धारित करना the size of the project;
- निर्धारित करना the technical and operational feasibility of alternative approaches;
- Assess (मूल्यांकन) लागत और लाभ of alternative approaches; and
- Report finding to the management with the recommendation explaining the acceptance or rejection of the proposal.

Phase 2: System Requirement Analysis

Thorough (सम्पुर्ण) and detailed (विस्तृत) understanding of the current system, **identifies the areas** that need modification to solve the problem, the **determination** of user/managerial **requirement** and to have fair idea about various systems development tools. Exact requirements of the user from the new system are specified.

What do you mean by system requirement analysis? What are the **activities to be performed** during system requirement analysis phase? **(May, 11)**

List the **activities to be performed** during the phase of System Requirement Analysis. **(May, 13)**

What are the major **objectives** of System Requirement Analysis phase in SDLC? (PM)

The following activities are performed in this phase **(RTP 14N)**

- To **identify and consult** the stake owners to determine their expectations and resolve their conflicts,
- To analyze requirements **to detect and correct** conflicts and determine priorities,

- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable.
- To **gather data or find facts** using tools like – interviewing, research/document collection, questionnaires, observation.
- To **model activities** such as developing models to document Data Flow Diagrams, E-R Diagrams
- To **document activities** such as interview, questionnaires, reports etc. and **development of a system (data) dictionary** to document the modelling activities,

(i)Facts Finding Technique

Discuss various facts finding techniques/ tools which are used by the system analyst for determining needs/requirement of the system to be built. **(MT –Nov, 14)**

What are the fact finding techniques used by a system analyst? **(Nov, 05)**

Briefly explain the various fact finding techniques which are used by the system analyst for determining the needs of an organization. **(NOV, 07)**

Detailed information is required **to determine "what are users' actual requirements**"? Various fact-finding techniques which are used by the system analyst for determining users' needs are discussed below:

- **Document:** Document means manuals, input forms, output forms, diagrams of how the current system works, organization charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the applications associated with the current system etc. Documents are a very good source of information about user needs and the current system. **They are easy to collect, convey a lot of information and provide relatively objective data.** The analyst should ensure that the documents which he is collecting are current, accurate and contain up-to-date information.
- **Questionnaires:** Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that **a large amount of data can be collected through a variety of users quickly**. Also, if the questionnaire is skillfully drafted, responses can be analyzed rapidly with the help of a computer.
- **Interview:** Users and managers may also be interviewed to extract information in depth. The data gathered through interviews **often provide systems developer with a complete picture of the problems and opportunities.** Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information. **and**
- **Observation** (अवलोकन)**:** In prototyping approaches, observation plays a central role in requirement analysis. Only by observing **how users react to prototype of a new system**, the system can be successfully developed. In traditional approach, the analyst should visit the user site to watch **how the work was taking place**. Such a surprise visit often helps the analyst in getting a clear picture of the user's environment and to determine why a request for a new system was submitted..

(ii)Analysis of Present System

Discus in brief the various functional areas to be studied by a system analyst for a detailed investigation of the present system. **(May, 11)**

What areas are required to be studied in order to know about the present system? **(Nov, 11) case study**

Describe any five functional areas of a system which needs to be analysed by system analyst for detailed investigation of the present system.(**MAY, 5)**

A Company is offering a wide range of products and services to its customers. It relies heavily on its existing information system to provide up to date information. The company wishes to enhance its existing system. You being an information system auditor, suggest how the investigation of the present information system should be conducted so that it can be further improved upon. **(MAY, 06)**

Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. Enough information should be assembled so that **a qualified person can understand the present system without visiting any of the operating departments**. Review of existing methods, procedures, data flow, outputs, files, inputs and internal controls should be intensive **in order to fully understand the present system and its related problems.**

- **Reviewing Historical Aspect:**
- **Analyzing Inputs:**
- **Reviewing Date Files:**
- **Reviewing Methods, Procedures, and Data Communications:**
- **Analyzing Outputs:**
- **Reviewing Internal Controls:**
- **Modelling the Present System:**
- **Undertake overall analysis of the PS:**

Review historical aspects: A brief history of the organization is a **logical starting point** for the analysis of the present system. The historical facts should identify the major turning points and milestones that have influenced its growth. A review of annual reports can provide an excellent historical perspective. A historical review of the organization chart can **identify the growth of management levels as well as the development of various functional areas and departments**. The system analyst should identify

what system changes have occurred in the past. These should include operations that have been successful or unsuccessful with computer equipment and techniques.

Analyze inputs: A detailed analysis of present inputs is important since they are **basic to the manipulation of data**. Source documents are used to capture the originating data for any type of system. The system analyst should be aware of the v**arious sources from where data can be initially** captured, keeping in view the fact that outputs for one area may serve as an input for another area. The system analyst must understand the nature of each form, what is contained in it, who prepared it, from where the form is initiated, where it is completed, the distribution of the form and other similar considerations. **If the analyst investigates these questions thoroughly, he will be able to determine how these inputs fit into the framework of the present system**.

Review data files maintained: The analysts should investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times per given time interval these are used. Information on common data files and their size will be an important factor, which will influence the new information system. This information may be contained in the systems and procedures manuals. The system analyst should also review all online and off ‐line files which are maintained in the organization **as these will reveal information about data that are not contained in any output**. The related cost of retrieving and processing data is another important factor that should be considered by the systems analyst.

Review methods, procedures and data communications: Methods and procedures **transform input data into useful output**. A method is defined as **a way of doing something**; a procedure is **a series of logical steps by which a job is accomplished**. A procedure's review is **an intensive survey** of the methods by which each job is accomplished, the equipment utilized and the actual location of the operations. Its basic objective is to **eliminate unnecessary** tasks or to perceive improvement opportunities in the present information system. A system analyst also needs **to review and understand** the present data communications used by the organization. He must review the types of data communication equipment including data interface, data links, modems, dial-up and leased lines and multiplexers. The system analyst must **understand how the data communications network** is used in the present system so as to identify the need to revamp the network when the new system is installed.

Analyze outputs: The outputs or reports should be scrutinized carefully by the system analysts in **order to determine how well they will meet the organization's needs**. The analysts must understand **what information is needed and why, who needs it and when and where it is needed.** Additional questions concerning the sequence of the data, how often the form reporting is used, how long it is kept on file, etc. must be investigated. Often many reports are a carryover from earlier days and have little relevance to current operations. Attempt should be made to eliminate all such reports in the new system.

Review internal controls: A detailed investigation of the present information system is not complete until internal controls are reviewed. **Locating the control points helps the analyst to visualize the essential parts and framework of a system**. An examination of the present system of internal control may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipment might allow much greater control over the data.

Model the existing physical system and logical system: As the logic of inputs, methods, procedures, data files, data communications, reports, internal control and other important items are **reviewed and analyzed in a top down manner**, **the process must be properly documented.** The logical flow of the present information system may be **depicted with the help of system flow charts**. The physical flow of the existing system may be shown by employing data flow diagrams. During the process of developing the data flow diagram, work on data dictionary for the new information system should be begun. **The data elements needed in the new system will often be found in the present system.** Hence, it is wise to start the development of the data dictionary as early as possible.

The flow charting and diagramming of present information not only organizes the facts, but also helps disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.

Undertake overall analysis of present system: Based upon the aforesaid investigation of the present information system, the final phase of the detailed investigation includes the analysis of:

- the present work volume
- the current personnel requirements
- the present benefits and costs
- Each of these must be investigated thoroughly.

(iii)System Analysis of Proposed System

(iv)System Development Tools

Many system development tools takes the form (रूप) of diagram (आरेख) or graphs (लेखाचित्र) representation. These tools help end users and system analyst **for the following;**

→ To conceptualize, clarify, document and communicate the activities and resources involved in the organisation and its Information system;

→ To analyze present business operations, management decision making and information processing activities of the organisation; and

→ To propose and design new or improved information system to solve business problems or **pursue business opportunities** that have been identified.

Major categories of tools

Q: Describe briefly four categories of major tools that are used for system development.

- **System Components and Flows,**
- **User Interface,**
- **Data Attributes and Relationship, and**
- **Detailed System Processes.**

A set of prominent tools are given below

- **Structured English**
- **Flowchart**
- **Data Flow Diagram**
- **Decision Tree**
- **Decision Table**
- **CASE Tools**
- **System Components Matrix**
- **Data Dictionary:**

How would you use Data Dictionary as a tool for file security and audit trails? **(May, 10)**

Write short Note on Data Dictionary **(May, 12)**, **(May, 05) (MAY, 07)**

A data dictionary is a computer file that contains descriptive information about the data items in the files of an IS. Thus, it is a computer file about data. Each computer record of a data dictionary contains information about a single data item used in the system. This information may include:

- ✓ Codes describing data item's length, data type and range.
- ✓ Identification of source documents used to create the data item.
- ✓ Names of the computer files that store the data item.
- ✓ Names of the computer programs that modify the data item.
- ✓ The identity of computer programs or individual permitted to access the data item for the purpose of the maintenance, upkeep or inquiry.
- ✓ The identity of computer programs or individual not permitted to access the data item.

❖ User Interface Layout Form

(v)System Specification

At the end of analysis phase, the System Analyst prepares a document called "Systems Requirement Specifications (SRS)". Write the contents of SRS. **(Nov, 11)**

As a part of system development team, the system analyst prepare a document called the System Requirement Specification" (SRS) . Describe the contents of SRS for a typical software development. **(May, 14)**

At the end of the analysis phase, the System Analyst prepares a document called "Systems Requirement Specifications (SRS)". A SRS contains the following:

- **Introduction:** Goals and Objectives of the software context of the computer-based system;
- **Information Description:** Problem description; Information content, flow and structure; Hardware, software, human interfaces for external system elements and internal software functions.
- **Functional Description:** Diagrammatic representation of functions; Processing narrative for each function; Interplay among functions; Design constraints.
- **Behavioral Description:** Response to external events and internal controls
- **Validation Criteria:** Classes of tests to be performed to validate functions, performance and constraints.
- **Appendix:** Data flow / Object Diagrams; Tabular Data; Detailed description of algorithms charts, graphs and other such material.
- **SRS Review:** It contains the following :
  - The development team makes a presentation and then hands over the SRS document to be reviewed by the user or customer.
  - The review reflects the development team's understanding of the existing processes. Only after ensuring that the document

represents existing processes accurately, should the user sign the document. This is a technical requirement of the contract between users and development team / organization.

(vi) Roles Involved in SDLC

Following are involved in the System Development Life Cycle (SDLC). Discuss their roles:

→ Project Manager
→ System Analyst
→ Database Administrator (DBA)
→ IS Auditor **(Nov, 11)**

Explain the role of auditor in information processing system design through SDLC. (**May, 14**)

- ✓ **Project Manager:** A project manager is normally **responsible for more than one project and liaisons with the client or the affected functions.** S/he is responsible **for delivery of the project within the time and budget** and periodically reviewing the progress of the project with the project leader and his/her team.
- ✓ **Systems Analyst:** The systems/business analysts' main responsibility is **to conduct interviews with users and understand their requirements**. S/he is a **link between** the users and the programmers to convert the users requirements in the system requirements and **plays a pivotal role** in the Requirements analysis and Design phase.
- ✓ **Database Administrator (DBA):** The data in a database environment has to be maintained by a specialist in database administration so as **to support the application program**. The DBA handles multiple projects; **ensures the integrity and security** of information stored in the database and also helps the application development team **in database performance issues**. **Inclusion of new data elements** has to be done **only with the approval** of the database administrator.
- ✓ **IS Auditor:** As a member of the team, IS Auditor **ensures that the application development also focuses on the control perspective.** He should be involved at the Design Phase and the final Testing Phase **to ensure the existence and the operations of the Controls in the new software**.

  RTP. **In SDLC**, some of the roles that an auditor has to perform are following:

  → To attend the project and steering committee meeting and examine project control documentation and conducting interviews in order to ensure what project control standards are to be complied with and determining the extent to which compliance is being achieved;
  → To examine the system documentation such as functional specifications to arrive at an opinion on the degree to which the system satisfies the general control objectives that any IS should meet;
  → To provide a list of the standards controls, over such operational concerns as response time, CPU usage, and random access space availability that the auditor has used as assessment criteria;
  → To rate various phases of SDLC on a rating system scale of 1 to10;
  → To provide control considerations that include documentation policy and procedures;
  → To determine if the expected benefits of the new system are realised and whether users are satisfied with the new system during the post implementation review etc.

Phase 3: System Design

Design describes the Parts of the system and their interaction. Design set out how the system shall be implemented using chosen hardware, software and network facilities. System design first involves logical design and then physical construction of the system. The logical design is like engineering blueprint; blueprint shows major features of the system and how they are related to one another. Physical construction **produces** program software, files and working system.

Design specification guides the programmers about "what the system should do and how to implement". The programmers, in turn, write the programs that accept input from users, process data, produces the report and store data in the files.

You have been associated with a system analysis team. Describe the important factors that you will consider while designing user input forms. **(Nov, 15)**
Discuss various issues that should be considered while designing systems input. **(Nov, 05)**
Discuss various issues that should be considered while designing system input. **(May, 08)**
(A)Architectural Design
(B) Design of Data/Information flow
(C)Design of Database **(Nov, 14) Q7** What are the major activities involved in the design of a database? **(May, 12)**
(D) User Interface Design
(E)Physical Design
(F) System Operating Platform
(G)Internal Design Controls

Various issues that should be considered while **designing systems input** are briefly discussed below:

Input design consists of **developing specifications and procedures** for data preparation, **developing steps** which are necessary to put transactions data into a usable form for processing, and data-entry, i.e., the activity of putting the data into the computer for processing.

A starting point for the input design process is **a review of the information compiled during the requirement analysis phase.** The analyst must review facts related to the current system such as what data are entered, who enters them, where they are entered, and when they are entered. This review **highlights basic problems and difficulties** with the present system. An understanding of the present system's input **directs attention to those areas needing improvement for more efficient data entry**.

(i) **Content:** The analyst is required to **consider the types of data** that are needed to be gathered **to generate the desired user outputs.** This can be **quite complicated** because the new system often means new information and new information often requires new sources of data. Sometimes, the **data needed** for a new system are **not available within the organization**. Hence, the system designer has to prepare new documents for collecting such information.

(ii) **Timeliness:** In data processing, it is very important that **data is inputted to computer in time** because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system. Timely input of data is very important in TPSs.

(iii) **Media:** Another important input consideration includes the **choice of input media** and subsequently the devices on which to enter the data. Various user input alternatives are available in the market such as **workstations, magnetic disc, OCR, pen-based computers and voice input** etc. A suitable medium may be selected depending on the application to be computerized.

(iv) **Format:** After the data contents and media requirements are determined, input formats are considered. While specifying the record formats, for instance, the **type and length of each data field** as well as any other **special characteristics** must be defined. Designing input formats often requires the assistance of a professional programmer or database administrator.

(v) **Input Volume:** Input volume refers to the **amount of data that has to be entered** in the computer system at any one time. In some decision-support systems and many real-time transaction processing systems, **input volume is light**. In batch-oriented transaction processing systems, **input volume could be heavy** which involves thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.

*What are the major activities involved in the design of a database? **(4 Marks, May 2012)**Or*

Write short note on Design of database. **(4 Marks, Nov. 2014)**

The designing of a database involves four major activities, which are given as follows:

- **Conceptual Modeling:** These describe the application domain via entities/objects, attributes of these entities/objects and static and dynamic constraints on these entities/objects, their attributes, and their relationships.
- **Data Modeling:** Conceptual Models need to be translated into data models so that they can be accessed and manipulated by both high-level and low-level programming languages.
- **Storage Structure Design:** Decisions must be made on how to linearize and partition the data structure so that it can be stored on some device. For example- tuples (row) in a relational data model must be assigned to records, and relationships among records might be established via symbolic pointer addresses.
- **Physical Layout Design:** Decisions must be made on how to distribute the storage structure across specific storage media and locations –for example, the cylinders, tracks, and sectors on a disk and the computers in a LAN or WAN.

System Acquisition

Technical Specifications and Standards

(a)Acquisition standards: Addresses the security and reliability issues.

(b)Acquiring Components From Vendors:

Acquiring appropriate hardware, and software is critical for the success of whole project. Management also describes whether the hardware is to be purchased, leased from a third party or to be rented.

Committee called 'System Acquisition Committee' is constituted.

Call for Request For Proposal (RFP) from vendors. RFP means asking vendors to submit proposals for the requirement mentioned. The following **considerations** are valid for both acquisition of hardware and software.

- Vendor selection: Prior to sending FRP.
- Geographical location of vendor: Local support person.
- Presentation by selected vendors: After technical validation, vendors are allowed to make presentation to the system acquisition team.
- Evaluation of Users feedback:

- ❖ Specific consideration
- ❖ The benchmark test

(c) Other Acquisition Aspects and Practices:

(i) Hardware acquisition
(ii) Software acquisition
(iii) Contracts, software licenses and copyright violations
(iv) Validating of vendors' proposals
(v) Methods of validating the proposal (CPPBT)
(a) Checklist:
(b) Point coring Analysis
(c) Public Evaluation Reports
(d) Benchmarking Problems related vendor's Solutions
(e) Testing Problem

Phase 4: System Development: Programming Techniques and Languages

To convert the design specification into a functional system under the planned operating system environments. Application programs are written, tested and documented, conduct system testing.

Characteristics of a Good Coded Program

What are the characteristics of a good coded program & application? **(MT –Nov, 14)** Discuss major characteristics of a good coded program in brief. **(PM)** What are the characteristics of a good coded program? **(Nov, 12)** Discuss the desired characteristics of a good coding system. (**MAY 2005)**

A good coded/written application and programs should have the following characteristics. (RE-RAUR)

- **Reliability:** It refers to the consistency with which a program operates over a period of time. However, poor setting of parameters and hard coding of some data could result in the failure of a 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 and outputs of a program even 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'. The second part becomes more challenging for quality control personnel and auditors.
- **Efficiency:** It refers to the performance per unit.
- **Usability:** It refers to a user-friendly interface and easy-to-understand internal/external documentation.
- **Maintainability:** It refers to the ease of maintenance of program even in the absence of the program developer and includes narrations in the source code.

Other related aspects of this phase;

(a)Program Coding Standards
(b)Programming Language
(c)Program Debugging: it is the most primitive form of testing activity which refers to correcting programming language syntax and diagnostic errors so that the programs compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by programmer into machine language instructions.
(d) Program Testing: A careful and thorough testing of each program is imperative to the successful installation of any system. The programmer should plan the testing to be performed, including testing of all the possible exceptions. The test plan should require the execution of all standard processing logic based on chosen testing strategy. It should be discussed with the project manager and/or system users. A log of test results and all conditions successfully tested should be kept. The log will prove invaluable in finding the faults and debugging.
(d)Testing Program
(e)Program Documentation
(f) Program Maintenance

Phase 5: System Testing *Explain **software testing** and state its objectives.**(November 2008)***

Testing is a process used to identify the correctness, completeness and quality of developed computer software. In other words, testing is nothing but CRITICISM or COMPARISON, i.e. comparing the actual value with expected one.

One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behaviour in reaction to the probing of the tester. The word testing means the dynamic analysis of the product—putting the product through its paces. Testing helps in verifying and validating if the software is working as it is intended to be working.

Objectives of Software Testing include:

- ➢ Testing is a process of executing a program with the intent of finding an error.

- A good test case is one that has a high probability of finding a yet undiscovered error. A successful test is one that uncovers a yet undiscovered error.
- The data collected through testing can also provide an indication of the software's reliability and quality. However, testing cannot show the absence of defect, it can only show that software defects are present.

(I)Unit testing:

What is unit testing? Explain five categorises of tests that a programmer typically performs on a program unit. **(PM)**
What are the categories of tests that a programmer typically performs on a program unit**? (Nov, 14)**
Testing a program unit is essential before implementing it. Name any four categories of test; a programmer typically performs on a programmable unit**. (May, 15)**
Describe the categories of tests that a programmer typically performs on a program unit. **(Nov, 15)**
Discuss the benefits and limitations of unit testing**. (May, 10)**

Ans: Programmer tests if individual unit of source code are fit for use. A unit is smallest testable part of an application. Written and run by the developer to ensure that code meets its design and behaves as intended.

Unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application, which may be an individual program, function, procedure, etc. or may belong to a base/super class, abstract class or derived/child class.

Unit tests are typically written and run by software developers to ensure that code meets its design and behaves as intended. The goal of unit testing is to isolate each component of the program and show that they are correct. A unit test provides a strict, written contract that the piece of code must satisfy.

There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

Categories of unit test (FPPSS)

- F: Functional: It check 'whether programs do, what they are supposed to do or not. **The test plan specifies** operating conditions, input values, and **expected result** and as per this plan, programmer checks by inputting the values to see **whether actual result and expected result match**.
- P: Performance: it is designed **to verify the** response time, execution time, the throughput, primary and secondary memory utilisation and traffic rate on data channels and communication links.
- S: Stress Test: It used to determine the stability of a given entity or system. Testing beyond normal operational capacity, often to breaking point, in order to observe the result.
- S: Structural Test:- it is concerned with **examining the internal processing logic** of a software system.
- P: Parallel test: The same test data is used in the old system and new system and the output result are then compared.

Technique of unit test

(a)Static testing (DSC)

Desk check: programmer checks for logical syntax errors and deviation from coding standards.
Structural walk through: The application developer leads other programmers to scan through the text of the program and explanation to uncover errors.
Code Inspection: The program is reviewed by a formal committee. Review is done with from checklist.

(b)Dynamic testing (BWG)

What are the difference between Black box & white box testing? **(MT Nov, 14)**

Black Box testing:

Briefly discuss Black Box Testing**.(Nov, 09)**
It takes an EXTERNAL perspective of the test object, to derive test cases. Functional or non-functional. Designer selects Typical inputs including simple, extreme, valid and invalid input-cases and execute to uncover errors. **(RTP 14N)**

Whit Box Testing**:** It **uses internal perspective** of the system **to design test cases** based on internal structure. **Require programming skills** to identify all paths through the software. The taster chooses test cases input **to exercise paths** through the code and **determine appropriate output**. Applicable at unit, integration and system level of the testing process, it is typically applied to the unit. **(RTP 14N)**

Gray Box testing:-

(II) Integration Testing:

Discuss integration testing and its types (**MT, 15M**)
Individual software modules are combined and tested as a group. This is carried out in following two manners;

- ❖ Bottom-up integration
- ❖ Top-down integration
- ❖ 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 and new control logic is invoked. These changes may cause problems **with function** that previously worked flawlessly. In the context of integration testing, RT ensures that changes or correction has **not introduced new faults**. The data used for RT should be the same as was used in the original test.

(iii) System Testing: Write short note on Types of System Testing **(Nov, 13) or** Discuss the system testing and its types**. (RTP 15M)**

Here Software and other system elements are tested as whole. The types of testing that might be carried out are as given; (RSSP)

- ✓ **Recovery**: - How well the application is able to recover from crashes, hardware failures and other similar problem. Forced failure of the software in variety of ways to verify that the recovery is liable to be properly performed, in actual disaster.
- ✓ **Security**: The process to determine that an IS protects data and maintains functionality as intended or not.
- ✓ **Stress** , and
- ✓ **Performance**: it is used to determine the speed or effectiveness of a computer or network, software program or device.

(IV)Final Acceptance Testing: To ensure that the new system meets/satisfies the quality standards adopted by the business and the system satisfies the users. It has two major parts; (QAUA)

- ➢ Quality assurance testing
- ➢ User acceptance testing
  - → Alpha testing
  - → Beta Testing

(V)Internal Testing Controls: To assure testing phase quality and efficiency.

Phase 6: System Implementation:

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

Explain different activities involved in conversion from manual system to computerized system. (**MAY 2005)**

Some of the key activities involved in System implementation include the following:

- ✓ **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 interval**.

Activities performed

(i)Equipment Installation –

- **Site Preparation**
- **Installation of new Hardware/software**
- **Equipment Checkout**

(ii)Training Personnel

(iii)System change-Over Strategies:

Explain the different conversion strategies used for conversion from a manual to a computerized system. **(May, 03)**

Explain different change over strategic used for conversion from old system to new system.(PM)

Describe various strategies for change over from manual system to computerised system.**(MAY 2006)**

The process of the changing over or shifting over from the old system to the new system. The four types of popular implementation strategies are described as follows:

- ❖ Direct implementation: An abrupt takeover (अचानक). This is achieved through an abrupt takeover – an all or no approach. With this strategy, the changeover is done in one operation, completely replacing the old system in one go.
- ❖ Phased Implementation: With this strategy, implementation can be staged with conversion to the new system taking place gradually.
- ❖ Pilot Changeover: With this strategy, the new system replaces the old one in one operation but only on a small scale. Any errors can be rectified or further beneficial changes can be introduced and replicated throughout the whole system in good time with least disruption.
- ❖ Parallel Changeover: This is considered as a secure method with both systems running in parallel over an introductory period. The old system remains fully operational while the new systems come online. With this strategy, the old and the new system are both used alongside each other, both being able to operate independently. If all goes well, the old system is stopped and new system carries on as the only system.

Discuss briefly the advantages and disadvantages of any one conversion strategy. **(May, 03)**

Advantages and disadvantages of most popular conversion strategy viz. Parallel conversion are discussed below:

Advantage: The advantage of running both systems is parallel includes the possibility of checking new data against old data in order to catch any errors in processing in the new system. Parallel processing also offers a feeling of security to users, who are not forced to make and abrupt change to the new system.

Disadvantage: It involves high cost of running two systems at the same time, and the burden on employee of virtually doubling their work load during conversion. Another disadvantage is that unless system being replaced is a manual one, it is difficult to make comparison between output of old system and new system. Suppose, the new system was created to improve on the old one. Therefore, the output from the system should differ. Finally, it is understandable that employees who are faced with a choice between two systems will continuing using the old one because of their familiarity with it.

(iv) Discuss briefly, various activities that are involved for successful conversion with respect to a computerised information system. **(May, 05)**

When the existing IS is to be converted into a new system, what are the activities involved in the conversion process?

It involves the following activities:

(a) Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually;
(b) Performing data cleansing before data conversion;
(c) Identifying the methods to assess the accuracy of conversion like record counts and controls totals;
(d) Designing exception reports showing the data which could not be converted through software; and
(e) Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

What activities are involved in system conversion? Explain them briefly. **(May, 13)**

Explain briefly various activities that should be completed for successful conversion of an existing system to the new information system. (**NOV, 07)**

Such requisites changeover or conversion includes all those activities, which must be complemented to successfully convert from the previous system to the new information system. **(PASS & Fail)**

→ **Procedures Conversion:**
→ **File Conversion:**
→ **System conversion:**
→ **Scheduling Personnel and Equipment:**
→ **Alternative plans in case of equipment failure:**

- **Procedures Conversion:** Operating procedures should be **completely documented** for the new system. This applies to both computer operations and functional area operations. **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, outputs, and internal controls must be **presented in clear, concise and understandable** terms for the average reader. **Written operating procedures** must be supplemented by **oral communication** during the training sessions on the system change. **Brief meetings** must be held when changes are taking place **in order to inform all operating employees** of any changes initiated. Revisions to operating procedures should be issued as quickly as possible. These efforts enhance the chances of successful conversion.
  Once the new system is completely operational, the system implementation group should spend several days checking with all supervisory personnel about their respective areas
- **File conversion:** Because large files of information must be converted **from one medium to another**, this phase should be **started long before** programming and testing are completed. The cost and related problems of file conversion are significant whether they involve on line files (common data base) or off line files. Present **manual files** are likely to **be inaccurate and incomplete** where **deviations** from the **accepted formats are common**. Computer generated files tend to be more accurate and consistent.
  In order for the conversion to be as accurate as possible, file **conversion programs** must be **thoroughly tested**. Adequate controls, such as **record counts and control totals**, should be the required output of the conversion program. The existing computer files should be **kept for a period of time** until the new system **perform in stable manner**. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.
- **System conversion:** After on line and off line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. **A cut off point is established s**o that data base and other data requirements can be **updated to the cutoff point**. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems. All differences must be reconciled. If necessary, appropriate changes are made to the new system and its computer programs. The old system can be dropped as soon as the data processing group is satisfied with the new system's performance.
- **Scheduling personnel and equipment:** Scheduling data processing operations of a new information system for the first

time is a difficult task for the system manager. As users become more familiar with the new system, however, the job becomes more routine.

Before the new design project is complete, it is often necessary to schedule the new equipment. Some programs will be operational while others will be in various stages of compiling and testing. Since production runs tend to push aside new program testing, the system manager must assign ample time for all individuals involved. Schedules should be set up by the system manager in co-ordination with departmental managers of operational units serviced by the equipment.

Just as the equipment must be scheduled for its maximum utilization, so must be personnel who operate the equipment. It is also imperative that personnel who enter input data and handle output data be included in the data processing schedule. Otherwise, data will not be available when the equipment needs it for processing.

- **Alternative plans in case of equipment failure:** Alternative-processing plans must be implemented in case of equipment failure. Who or what caused the failure is not as important in case of equipment failure as the fact that the system is down. Priorities must be given to those jobs critical to an organization, such as billing, payroll, and inventory. Critical jobs can be performed manually until the equipment is set right.

  Documentation of alternative plans is the responsibility of the computer section and should be fully covered by the organization's systems and procedures manual. It should state explicitly what the critical jobs are, how they are to be handled in case of equipment failure, where compatible equipment is located, who will be responsible for each area during downtime and what deadlines must be met during the emergency. A written manual of procedures concerning what steps must be undertaken will help to overcome the unfavorable situation. Otherwise, panic will result in use of the least efficient methods when time is of the essence.

Phase 6: Post Implementation Review and System Maintenance

Post Implementation Review

It answers 'Did we achieve what we set out to achieve in business term'? It ascertains degree of success achieved from the project. It examines the efficacy of all elements of the working solution to see if further improvement can be made to optimise the benefit derived. It should be scheduled sometime after solution has been deployed.

What are the **activities** to be undertaken during the Post Implementation Review? **(Nov, 12)**

"The final step of the system implementation is its evaluation." What functions are being served by the system evaluation? Discuss development, operation and information evaluations. **(Nov, 04)**

What is the purpose of the system evaluation? How is it performed? **(May, 08)**

Evaluation provides feedback necessary to assess the value of information and the performance of personnel and technology included in the newly designed system. These feedbacks serves two functions:

- It provides information as to what adjustment to the IS may be necessary.
- It provides information as to what adjustment should be made in approaching future IS development project.

Two aspects of IS should be evaluated.

- 1st aspect is whether the newly developed system is **operating properly**.
- 2nd aspect is whether user is **satisfied with** the IS with regard to reports supplied by it.

Typical evaluation includes the following (DIO)

- Development Evaluation: Whether the system was developed on schedule and within budget.
- Operational Evaluation: Whether the hardware, software and personnel are capable to perform their duties.
- Information Evaluation: The extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system.

- ✓ **Development Evaluation:** Evaluation of the development process is **primarily concerned with** whether the system was developed on schedule and within budget. This is a **rather straightforward** evaluation. It **requires** schedules and budgets to be established **in advance** and that record of actual performance and cost be maintained. It may be noted that **very few information systems have been developed on schedule and within budget**. In fact, many information systems are developed **without clearly defined schedules or budgets**. Due to the uncertainty and mystique associated with system development, they are **not subjected to traditional management control procedures.**
- ✓ **Operation evaluation:** The evaluation of the information system's operation **pertains to** whether the hardware, software and personnel are capable to perform their duties and they do actually perform them so. **Operation evaluation answers such questions:**
  A. Are all transactions processed on time?
  B. Are all values computed accurately?
  C. Is the system easy to work with and understand?
  D. Is terminal response time within acceptable limits?
  E. Are reports processed on time?
  F. Is there adequate storage capacity for data?

Operation evaluation is **relatively straightforward** if evaluation **criteria** are established **in advance**. For example, if the systems analyst lays down the criterion that a system which is capable of supporting one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.

- ✓ **Information evaluation:** An information system should also be evaluated **in terms of information it provides**. This aspect of system evaluation is **difficult** and it cannot be conducted **in a quantitative manner**, as is the case with development and operation evaluations. **The objective** of an information system is **to provide information to support** the organizational decision system. Therefore, **the extent to which information provided** by the system is **supportive to decision making** is the area of concern in evaluating the system. However, it is **practically impossible** to directly evaluate an information system's support for decision-making in an organization. It must be **measured indirectly**. User satisfaction can be used **as a measure to evaluate** the information provided by an information system. Measurement of user satisfaction can be accomplished using the interview and questionnaire technique. **If management is generally satisfied with an information system, it is assumed that the system is meeting the requirements of the organization. If management is not satisfied**, **modifications ranging from minor adjustments to complete redesign may be required.**

System Maintenance (updates)

Short note on Information System Maintenance **(Nov, 11)**
Briefly explain about various categories of software maintenance used in System Development Life Cycle (SDLC). **(May, 14)**
Write short notes on System maintenance. **(Nov, 05)**
Write short notes on System maintenance **(MAY, 07)**

System Maintenance: Most information systems require **at least some modification after development**. The need for modification arises from **a failure to anticipate** all requirements during system design and/or from changing organizational requirements. The changing organizational requirements continue to impact most information systems as long as they are in operation. Consequently periodic systems maintenance is required for most of the information systems. Systems maintenance involves adding new data elements, modifying reports, adding new report, changing calculation etc.

Maintenance can be categorized in the following two ways:

(a) Scheduled maintenance is anticipated and can be planned for. For example, the implementation of a new inventory coding scheme can be planned in advance.

(b) Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested should have few occasions of rescue maintenance.

. Categorise of maintenance

(CAPS is at Ramdash Peth)

- ❖ Corrective Maintenance: It deals with fixing bugs in the codes or defect found during execution. (PM)
- ❖ Adaptive Maintenance: Adapting software to changes in the environment. (PM)
- ❖ Preventive Maintenance: Aimed at increasing the system's maintainability.
- ❖ Scheduled Maintenance: इसे anticipate किया जाता है और plan भी कर सकते है।
- ❖ Rescue Maintenance: Previously undetected malfunction जो anticipate नहीं किए गए थे।
- ❖ Perfective Maintenance: It deals with accommodating to the new or changed users requirement.

Various categories of software maintenance are given as follows:

→ **Scheduled maintenance:** Scheduled maintenance is anticipated and can be planned; for example, implementation of a new inventory coding scheme can be planned in advance.

→ **Rescue maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate solution. A system that is properly developed and tested, should have few occasions of rescue maintenance.

→ **Corrective maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found. A defect can result from design errors, logic errors; coding errors, data processing and system performance errors.

→ **Adaptive maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The need for adaptive maintenance can only be recognized by monitoring the environment.

→ **Perfective maintenance:** Perfective maintenance mainly deals with accommodating to new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.

→ **Preventive maintenance:** Preventive maintenance concerns activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

Operational manual

User's Guide. Technical communication document intended to give assistance to the people using a particular system. The sections of operation manual are

Auditors' Role in SDLC
Three objectives

Computer Software
Definition: Software is a set of programs, which is designed to perform **a well defined function**. A program is **a sequence** of instruction written to solve **a particular problem**.
Types of software

1. Application software
2. System Software

System software- the system software is a collection of programs designed to operate, control and extend the processing capabilities of the computer itself. System software is generally prepared by computer manufacturer.
Application Software: Applications software are the software that are designed **to satisfy a particular need** of a particular environment. All software prepared by us in the computer lab. Example: Student record software, railway reservation software, income tax software, word processor etc

Chapter 6: Audit of Information System

Needs for audit of information systems

Discuss the impact of IS audit on the organisation. (MT Nov, 14),
What are the factors influencing an organisation towards controls and audit of computers? **(Nov, 15)**
Factors affecting an org^{n} toward controls and audit of com^{r} and the **impact** of Information systems on audit function on org^{n} are

- **Organisation cost of Data Loss**: Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **High cost of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **Cost of Incorrect Decision Making**: Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions **require accurate data to make quality decision** rules.
- **Cost of Computer Abuse:** These are **critical resources** of an organisation, which has **a credible impact** on its infrastructure and business competitiveness.
- **Value of Hardware, Software, Personnel** : Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **Maintenance of Privacy**: Today, data collected in a business process contains private information about an individual too.
- **Controlled evolution of computer use:** Use of **Technology and reliability of complex computer systems cannot be guaranteed** and the consequences of using unreliable systems can be destructive.

Information System Auditing

- Improved **Safeguard** of Assets
- Improved Data **Integrity**
- Improved System **Effectiveness**
- Improved System **Efficiency**

Effect of computer on audit
Q. Impact of technology on Internal Controls. (**MT Nov, 14**)
(i)Change to evidence **collection**
(ii) Changes to Evidence Evaluation
(i)Change to evidence **collection** (DAN LAL) **(RTP 14N) (May, 15),**

Compared to traditional audit, evidence collection has become more challenging with the use of the computer to the auditor. What are the issues which affect evidence collection and understanding the reliability of control of financial audit? **(Nov, 14)**

- ✓ **D: Data Retention and Storage**: Storage capacity might **restrict** the amount of **historical** data that can be retained "on-line" and readily accessible to the auditor. Insufficient storage capacity may not allow the auditor to review the whole reporting period transaction on the CS.
- ✓ **A: Absence of Input Document:** Transaction may be entered into computer system without the presence of supporting document. The increasing use of EDI will result in less paperwork available for audit examination.
- ✓ **N: Non Availability of Audit Trail**: AT in some CS may exist only for short period of time. Non-availability of AT will make auditor job very difficult & auditor will have to carry out audit using approach called audit around the computer.
- ✓ **L: Lack of Availability of Output:** The result processing may not produce a hard copy output form output. Non-availability of hard copy output makes it necessary for the auditor to directly access the E-data retained in client's computer.
- ✓ **A: Audit Evidence:** Transaction may be generated automatically by the CS.
- ✓ **L: Legal Issue**: Use of computer for carrying out trading activities. This can create problems with the contract, e.g. when is the contract made, where is it made, what are the terms of contract and who are the parties to the contract.

(ii) Changes to Evidence Evaluation: Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system.

- ❖ **System generated transactions:** Financial systems may have the ability to initiate, approve and record financial transactions.
- ❖ **Automated transaction processing** systems can **cause the auditor problems**. For example when gaining assurance that a transaction was properly authorised or in accordance with delegated authorities. These are frequently used in JIT inventory and stock control systems: When a stock level falls below a certain number, the system automatically generates a purchase order and sends it to the supplier.
- ❖ **Systemic Error:** Computers are designed to **carry out processing on a consistent basis**. Given the same inputs and programming, they invariably produce the same output. This consistency can be viewed in both a positive and a negative manner.

The IS audit

The IS Audit of an IS environment may **include one or both of the following**:

→ Assessment of internal controls within the IS environment to assure **validity, reliability, and security** of information and ISs.

→ Assessment of the **efficiency and effectiveness** of the IS environment.

What is the sole purpose of an Information System audit? **(Nov, 3)**

The sole purpose of an Information system audit is **to evaluate and review** the adequacy of automated information systems **to meet processing needs**, to evaluate the adequacy **of internal controls**, and to ensure that assets controlled by those systems are **adequately safeguarded**.

Responsibility of IS Auditor

What is the skill set expected from an IS auditor? **(Nov, 12)**
Explain the set of skill that is generally expected of an IS auditor. **(Nov, 12)**

Whatever is expected from the auditor, is the responsibility of IS auditor. The set of skill generally expected to be possessed by the IS auditor include;

- ➢ Sound knowledge of business operations, practices and compliance requirement;
- ➢ Should possess the **requisite professional technical qualification**;
- ➢ A good understanding of **information risks and controls**;
- ➢ Knowledge of IT **strategies, policy and procedural control**;
- ➢ Ability to understand **technical and manual controls** relating to business continuity;
- ➢ Good knowledge of **professional standards and best practice** of IT controls and security.

Function of IS Auditor

As an IS auditor, what are **the risk reviewed** by you relating to IT System & processes as part of your functions**?** **(Nov, 14)**
In this company, what are your function as an IS auditor? **(Nov, 15)**

IS auditor review risk relating to IT systems and processes; some of them are:

- ❖ **Inadequate** information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.),

- **Inefficient** use of resources, or poor governance(e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.),
- **Ineffective** IT strategies, policies and practices (including a lack of policy for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.) , and
- IT related **frauds**(including phishing, hacking etc).

What is the role of IS auditor? **(Nov, 03)**

The Information System (IS) auditor is responsible **for establishing control objectives** that reduce or eliminate potential exposure to control risks. **After** the objectives of the audit have been **established**, the auditor must **review the audit subject** and **evaluate the results of the review to find out areas that need some improvement**. IS auditor should **submit a report to** the management, **recommending actions** that will **provide a reasonable level of control over the assets of the entity**.

Categories of IS Audits (SISMT)

Discuss the various categories of IS Audit **(MT- N0v,14) (RTP 15M)**

What is the scope of IS audit process? Explain the categories of IS audit**. (Nov, 12)**

The scope of IS Audit process should include the examination and evaluation of the adequacy and effectiveness of the system of internal controls and the quality of performance by the information system. In addition, IS Audit process will also examine and evaluate the planning, organizing, and directing processes to determine whether reasonable assurance exists so that objectives and goals will be achieved. Such evaluations, in the aggregate, provide information to appraise the overall system of internal control.

The scope of the audit will also include the internal control system/s for the use and protection of information and the information systems, such as, *Data, Application systems, Technology, Facilities, and People.*

IS Audit has been categorized into the following five major types: (SIS-MT)

- S: **System and Application Audit**: An audit **to verify,** that S&A are appropriate, adequate and adequately controlled **to ensure** timely, reliable, accurate and secure input, processing and output at all the level of a system's activity.
- **I: Information Processing Facilities**: An audit **to verify that** the processing facility is controlled **to ensure** timely, accurate and efficient processing of applications **under normal and potentially disruptive conditions.**
- **S: System Development**: An audit **to verify** that the system under development meet the objective of the organisation and **to ensure** that the systems are developed in accordance with generally accepted standards for the system development.
- **M: Management of IT and Enterprise Architecture**: An audit **to verify** IT management has developed an organisational structure and procedures **to ensure** a controlled and efficient environment for information processing.
- **T: Telecommunication, Intranet and Extranet:** An audit **to verify** that controls are **in place** on the client, server and the on the network connecting the clients and servers.

Steps in IS audit

Different auditors go about IS auditing in different ways. Despite this, IS audit process can be categorized into broad categories. Discuss the statement explaining broad steps involved in the process**. (May, 15)** (6 Marks)

As an IS Auditor, what are the steps to be followed by you while conducting IT auditing? **(May,12)**

(a) **Scoping**: Determine **main areas of focus** and any areas which are explicitly **out of scope**, based on **scope definition** agreed with management.

(b) **Planning**: The **scope** is broken down into greater level of detail, usually involving the generation of an audit work plan.

(c) **Fieldwork**: Gathering evidence by interviewing staff and manager, reviewing document and process.

(d) **Analysis**: Disparately **sorting out, reviewing and trying to make sense** of all that evidence gathered earlier. SWOT and PEST.

(e) **Reporting**: It is done after analysis of evidence gathered and analysed.

(f) **Closure:** Preparing notes **for future audits** and follow up with management to complete the actions they promised after previous audit.

Audit standard and best practices

- ISCA

- IS audit standards: 16, define the mandatory requirement for IS audit. Auditor shall comply.
- IS audit guidelines: 39, provide a guideline in applying IS auditing standards.
- IS audit procedure: 11, provide example of procedure an IS auditor need to follow while conducting IS audit for complying with IS audit standards.
- COBIT: Containing Good business practices relating to information technology.

❖ ISO27001: A systematic approach to manage INFORMATION SECURITY in an IS environment.
❖ Internal Audit Standards
❖ Standards on Audit Issued by ICAI
❖ ITIL: A set of practice for IT Service Management that focuses on aligning IT service with business need.

Performing IS Audit

Audit planning concept: Materiality and significance; risk based approach of audit planning.
Basic plan:

Preliminary review: KULUR

a. **Knowledge of business**; Related aspects are given as follows:
   © General **economic factors and industry conditions** affecting the entity's business,
   © Nature of Business, its products & services,
   © General **exposure** to business,
   © Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced,
   © Level of **competence of the Top management** and IT Management, and
   © Finally, **Set up and organization** of IT department.

b. **Understanding of technology;(QPM**)
   You are appointed to audit the Information Systems of ABC Limited. As a part of preliminary evaluation, list the **major aspects which you would study** to gain a good understanding **of the technology environment and the related control issues. (May, 15)**
   An important task for the auditor as a part of his preliminary evaluation is to **gain a good understanding of the technology environment and related control issues**. This could include consideration of the following:
   - ❖ Analysis of business processes and **level of automation**,
   - ❖ Assessing the **extent of dependence** of the enterprise on IT **to carry on its businesses** i.e. Role of IT in the success and survival of business,
   - ❖ Understanding **technology architecture** which could be quite diverse such as a distributed or a centralized or a hybrid **architecture**,
   - ❖ Studying **network diagrams** to understand **physical and logical** network **connectivity**,
   - ❖ Understanding **extended enterprise architecture** wherein the organization systems **connect seamlessly** with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
   - ❖ Knowledge of **various technologies** and their **advantages & limitations** is a critical **competence requirement** for the auditor. For example, authentication risks relating to e-mail systems,
   - ❖ And finally, Studying IT policies, standards, guidelines and procedures.

c. Legal consideration and audit standards; and
d. **Understanding internal control systems**
e. **Risk assessment and materiality: .**

Risk Based approach to make Audit Plan: The steps that can be followed for a **risk-based approach** to make an audit plan are given as follows:

❖ **Inventory** the ISs **in use** in the organization and **categorize them**.
❖ **Determine** which of the systems **impact critical functions or assets**, such as money, materials, customers, decision making, and how close to real time they operate.
❖ Assess **what risks affect** these systems and **the severity of the impact on the business**.
❖ Based on the above assessment, **decide** the audit **priority**, resources, schedule and **frequency**.

Audit risk is the product of followings:

Audit risk can be defined as the risk **that the information**/financial report may **contain** material **error** that may go **undetected** during the course of the audit.

Q. Difference between Control risk and Detection risk. (**MT 15M**)

➢ **Inherent Risk:**

- **Control Risk**: Risk that the error or omissions are **not detected or corrected** on timely manner **by entity's internal control**.
- **Detection Risk:** Risk that the **auditor Substantive Procedure** will not be able to detect any error or fraud.

IS audit and audit evidence

SA-230, audit documentation refers to the **record** of audit procedure performed, relevance audit evidence collected and the conclusions the auditor reached.

Documentation by auditor: SA-200 prescribes Inherent limitations of an audit.

Provision relating to digital evidence: Indian Evidence Act, 1872 and Information Technology Act, 2000. Now electronic record is accepted as evidence in the court of law.

Concurrent or continues audit:

"In on-line systems, conventional audit trail is difficult and almost impossible". Why? Explain the kind of audit techniques used in such system. **(Nov, 04)**

Historically, auditors have placed substantial reliance in evidence-collection work on the paper trail that documents the sequence of events that have occurred within an information system. Paper based audit trails have been progressively disappearing as online computer -based systems have replaced manual systems and as source documents have given a way to screen based inputs and outputs. In a batch processing system, one can still expect to find a visible trail of "run -to -run "controls, which can be reconciled to the original input batch totals. In such systems, it is unusual to find any significant loss of audit trails regarding the control totals. In online systems, however, data are stored in device-oriented rather than human-oriented form. Moreover, data files belonging to more than one application may be updated simultaneously by each individual transaction. In such systems, traditional run-to-run controls do not exist and the potential for loss of audit trail is significant.

In a batch processing systems, the test data is prepared by an auditor for audit purposes and the results are obtained from the program under execution and copy of relevant files. The results are compared with the predetermined correct outputs. Any discrepancies indicating processing errors or control deficiencies etc. are thoroughly investigated. In on-line systems, such kind of audit trail is not desirable since millions of transactions can be processed in a short time. In such cases, evidence gathered after data processing is insufficient for audit purposes. In addition, since many on-line systems process transactions continuously, it is difficult or impossible to stop the system in order to perform audit tests. Hence, the auditor needs to identify problems that can occur in an information system on a more timely basis. For this reason, a set of audit techniques has been developed to collect evidence at the same time as an application system undertakes processing of its production data.

Concurrent Audit Techniques: These techniques can be used **to continually monitor the system and collect audit evidence** while live data are processed during regular operating hours. As the name suggests, this type of audit technique **uses embedded audit modules**, which are segments of program codes that perform audit functions. **They also report test results to the auditors and store the evidence collected for the auditor's review.** These techniques are often **time consuming and difficult to use**, but are less so, if incorporated when programs are developed.

There are five such techniques, which auditors commonly use.

- **Information Systems Control and Audit**
- **Integrated Test Facility (ITF):**
- **Snapshot Technique:**
- **SCARF:**
- **Audit Hooks:**
- **CIS:**

It is used when documents are available only in digital form. To prepare proper audit report auditor needs documented audit evidence. Therefore, auditor will use CAT for collecting audit evidence and documenting audit evidence in online and real time system.

- **Snapshot**: This technique examines the way transactions are processed. Selected transactions are marked with special code that triggers the snapshot processes. Audit modules in the program record these transactions and their master file records before and after processing. Snapshot data are recorded in a special file and reviewed by the auditor to verify that all processing steps have been properly executed. **(RTP 14N)**
- **Integrated test facility:**

'Real time information system needs real time audit techniques like Integrated Test Facility (ITF) to provide continuous assurance.' Define and explain the ITF methodology. **(Nov, 13**

Write short notes on Integrated test facility **(May, 04)**

Write short notes on Integrated Test Facility **(NOV, 2006)**

This is one of the concurrent audit techniques **which places a small set of fictitious records in the master files.** The records might represent **a fictitious division**, department, or branch office or a customer or supplier. Processing test transactions to update these dummy records will not affect the actual records. Because fictitious and actual records are processed together, company employees usually remain unaware that this testing is taking place. The system must distinguish ITF records from actual records, collect information on the effects of the test transactions, and report the results. The auditor compares processing and expected results in order to verify that the system and its controls are operating correctly.

In a batch processing system, the ITF technique eliminates the need to reverse test transactions and is easily concealed from operating employees. ITF is well suited to testing on-line processing systems because test transactions can be submitted on a frequent basis, processed with actual transactions, and traced throughout every processing stage. All this can be accomplished without disrupting regular processing operations. However, care must be taken not to combine dummy and actual records during the reporting process.

Creation of **dummy entity** in the application system files and **the processing** of audit test data against the dummy entity **as means of verifying** processing authensity, accuracy and completeness. Method of entering test data and methods of removing the effect of ITF transaction.

- **System controlled audit review file:** It involves **embedding** Audit Software Module within a Host Application System **to provide continuous monitoring** of the system transactions. The information collected is **written onto a special file**. Auditor then **examines** the information contained on the file **to see if some aspect of the application system need follow-up. (RTP-15M).**

Types of information that can be collected using SCRAF. (RTP 14N)

As an IS auditor, explain the types of information collected for auditing by using SCRAF technique. **(May, 11) or** What do you mean by "SCRAF"? What types of information can be collected by auditor using SCRAF? **(May, 13)**

- © **Application System Error:** SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- © **Policy and procedural variance**: Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- © **System Exception, Statistical Sample:** SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- © **Snapshot and extended records:** Snapshots and extended records can be written into the SCARF file and printed when required.
- © **Statistical Sampling**: Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- © **Profiling data:** Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- © **Performance Measurement**: Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

- **Continuous and Intermittent Simulation**: Write short notes on Continuous and Intermittent Simulation (CIS) **(May, 14)**

This is a variation of the System Control Audit Review File (SCARF) continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system. During application system processing, CIS executes in the following way:

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

- **Audit hooks**: These are audit routines that flag suspicious transactions. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach, known as "real-time notification", displays

a message on the auditor's terminal.

Advantage and disadvantages of CATs

Describe major advantage of CATs (**May, 05 + MT-Nov, 14**)
Describe the Advantage and disadvantages of CATs in brief. **(Nov, 11)**
Describe some of the advantages of continuous audit techniques. **(May, 10)**
Briefly describe the advantages and disadvantages of continuous auditing techniques. **(May, 14)**
List-out and explain the advantage of using CAT for the proposed system**. (Nov, 15)**

- **Timely, Detailed and Comprehensive Audit**: Evidence will be available more timely and in a comprehensive manner. 100% processing can be evaluated and analysed **rather than** examining the input and output only.
- **Surprise test capability**: As the evidences are collected from the system itself by using CAT, auditor can gather evidence **without** the system staff and AS user being aware that the evidence is being collected at that particular moment.
- **Information to the system staff on meeting of objective:** CAT provides information to the system staff **regarding the test vehicle to be used** in evaluating whether an AS meets the objective of asset safeguarding, data integrity, effectiveness and efficiency.
- **Training for new users:** Using ITF, new user can submit data to the AS, and obtain feedback on any mistakes they make via the system's error reports.

Potential benefits

Disadvantage/Limitation of CAT

→ Auditor will be able to **obtain resources required** from the organization to support DIO&M of CAT.
→ CAT is more likely to be used **if the auditors are involved in development** work associated with an NEW AS.
→ Auditors **need the knowledge and experience of working with CS** to be able to use CAT effectively and efficiently.
→ CAT is more likely to be used **where the audit trail is less visible and the costs of errors** and irregularities are high.
→ CAT is not likely to be effective unless they are implemented **in an AS that is relatively stable.**

Audit trail (RTP 15M)

Audit trails are logs (register) that can be **designed to record activity** at the system, application and user level.

Audit Trail Objectives (PDF)

(i) Discuss the various ways in which audit trail can be used to support security objectives. **(Nov, 05)**
(ii) How audit trail can be used to support security objective? (**MT –Nov, 14)**
(iii) In what ways, an audit trails is used to support security objectives? Describe each one of them. **(Nov, 11)**

- **P: Promoting Personal Accountability**: cab be used to monitor user activity at the lowest level of detail. It is preventive control used to influence user behaviour.
- **D: Detecting Unauthorised Access to the System**: Real time (RT) or after the fact detection (AFD). Objective of the RTD is to protect the system from outsider trying to breach the system control. RTD impose significant overhead on the OS, can degrade the operational performance. AFD logs can be **stored electronically** and **reviewed periodically or as needed**
- **F: Facilitating the Reconstruction of Events**: It can be used to reconstruct the STEPS that led to EVENTS. Knowledge of condition existed at the time of system failure can be used to avoid similar situation in the future.

Implementing audit trail

General controls

What are the **key things** that an auditor needs to consider while evaluating **the application and general controls**?
Various general controls are given as follows

a. Operating system controls
b. Data management controls
c. Organisational Structure Controls
d. System development Controls
e. System maintenance Controls
f. Computer Centre Security Controls
g. Internet and internet controls

Application controls: These are categories in the following types. (IPO)

- ❖ Input controls
- ❖ Processing controls
- ❖ Output controls

Data management controls

These controls fall in two categories

(1) Access controls: designed to prevent unauthorised individual from viewing, retrieving, computing or destroying the entity data. Manner in which control is established; (I) User Access Controls through passwords, tokens and biometric controls; and (II) Data Encryption controls: Keeping data in database in encrypted form.

(2) Back up controls (Copies of data): Ensure availability of data in the event of data loss due to unauthorised access, equipment failure or physical disaster and entity can RETRIEVE its file and databases.

Various backup **strategies** are given as follows. (Just remember DPLL)

D: Dual recording of data:	2 complete copies of database are maintained
P: Periodic dumping of data:	Taking a PERIODIC dump of all or part of the DB. DB is saved at a point in time by copying DB onto some backup storage medium. The dump may be scheduled.
L: Logging input transactions	Logging the input data transactions **which cause changes to the DB**. Work in conjunction with a periodic dump. In case of complete DB failure, the last dump is loaded and transactions, which are logged since the last dump.
L: Logging changes to the data	Copying a record **each time it is changed** by an update action. Changed record can be logged immediately before the update action changes the record, after or both.

Audit of Evaluation techniques for physical and Environmental Controls.

Role of IS auditor in Physical Access controls: Risk Assessment, Controls Assessment, and Review of Documents. RA, CA and RD.

Audit of Environmental Controls

a. Role of auditor in Environmental Controls,
b. Audit planning and assessment,
c. Audit of environmental controls, and
d. Documentation.

Audit of Application Security Controls

The objective of this exercise is to establish whether the application security controls are operating effectively to protect the CIA of information.

Approach to application security audit:

Auditor needs to have a clear understanding of the following;

- ❖ Business process for which application has been designed;
- ❖ The source of data input to the application;
- ❖ The output from application;
- ❖ The various interface of the application under audit with other applications;

Brief understanding of various layers

- ❖ Operating layer
- ❖ Tactical Layer
- ❖ Strategic layer

Operating layer

Major audit issues at the operational layer

User account & Access Right	Defining **unique user accounts** and providing them access rights **appropriate** to their roles and responsibilities. Auditor needs to always ensure **the use of unique user Ids**, these needs to e traceable to individual for whom they are created.
Password Controls	In general, password strength, p minimum length, p age, p non-repetition and automated lockout **after 3 attempts should be set as a minimum**. Auditor needs to check whether there are applications where password controls are weak.
Segregation of duties	Segregation of duties is a basic internal control that prevents or detects errors and irregularities **by assigning responsibility** for initiating and recording transactions and custody of assets **to separate individual**.

Chapter 7: Information Technology Regulatory Issues Information Technology Act, 2000;

Legal Recognition of Electronic Evidence i.e. digital evidence through chapter iii of IT Act, 2000 its impacts;

- ❖ Indian Evidence Act, 1872 has been amended to give legal recognition of digital evidence therefore court will have to accept digital evidence during prosecution. Cyber Forensic;
- ❖ Audit Evidence: SA 200 'OVERALL OBJECTIVES OF THE INDEPENDENT AUDITOR AND THE CONDUCT OF AN AUDIT IN ACCORDANCE WITH STANDARDS ON AUDITING among other things require the auditor to "Form an opinion on the financial statements based on conclusions drawn from the audit evidence obtained". Therefore with the

legal recognition of electronic evidence auditor has legal right to rely on digital evidence to form his opinion on true and fairness view of financial statement.

Section 7: Retention of Books of Account in electronic form thus removing the need to retain it in physical form.

Some of the key issues of Electronic Information impacting auditors and enterprises are;

- **Authensity**: How do we implement a system that ensures that transactions are genuine and authorised?
- **Reliability**: How do we rely on the information, which does not have physical documents?
- **Accessibility**: How do we access and authenticate this information, which is in digital form?

Objectives of the IT Act, 2000

Objectives of Information Technology Act 2000 **(May, 12)**

State the objectives and scope of IT Act, 2000. (**MAY 2005)**

Write short notes on Objectives of Information Technology Act, 2000. (**NOV, 07)**

Major objectives of the Information Technology Act 2000 are given as follows:

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
- To facilitate electronic filing of documents with Government departments; To facilitate electronic storage of data;
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- To give legal recognition for keeping of books of accounts by banker's in electronic form; and
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

Scope of the Act: This Act is applicable to whole of India, unless otherwise provided in the Act. It also applies to any offence or contravention there under committed outside India by any person.

Different provisions of this Act came into force on the different dates as notified by the Central Government.

The Act shall not be applicable to the following:

- a negotiable instrument as defined in Section 13 of the Negotiable Instruments Act, 1881;
- a Power of Attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882;
- a trust as defined in Section 3 of the Indian Trusts Act, 1882;
- a will as defined in Section (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
- any contract for the sale or conveyance of immovable property or any interest in such property;

Any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Define the following terms related to Information Technology Act, 2000:

- Computer contaminant
- Cyber Café
- Electronic form
- Traffic data
- Asymmetric crypto system **(May, 10)**

(1) Computer Contaminant: It refers to any set of computer instructions that are designed: to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or by any means to disrupt the normal operation of the computer, computer system, or computer network.

(2) Cyber Cafe: It refers to any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.

(3) Electronic Form: It refers to any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

(4) Traffic Data: It refers to any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, data size, duration or type of underlying service or any other information.

(5) **Asymmetric crypto system:** It refers to a system of secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Define the following important terms in the light of the Section 2 of the I.T. Act, 2000:

- ✓ Affixing digital signature

- ✓ Asymmetric crypto system
- ✓ Computer network
- ✓ Private and Public keys
- ✓ Secure system. **(Nov, 04)**

The definition of important terms according to Section 2 of the Information Technology Act, 2000 is as under:

(i) **"Affixing digital signature"** with its grammatical variation and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.

(ii) **"Asymmetric crypto system"** means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

(iii) **"Computer network"** means the interconnection of one or more computers through –

(a) the use of satellite, microwave, terrestrial line or other communication media; and

(b) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

(iv) **"Private and public keys"** refer to a key pair used in an asymmetric crypto system. Private key means the key used to create a digital signature whereas public key is used to verify the same and is listed in the Digital Signature Certificate.

(v) **"Secure system"** means computer hardware, software and procedures that

- ➢ are reasonably secure from unauthorized access and misuse;
- ➢ provide a reasonable level of reliability and correct operation;
- ➢ are reasonably suited to performing the intended functions; and
- ➢ adhere to generally accepted security procedures.

What are the conditions subject to which electronic record may be authenticated by means of affixing digital signature? **(June, 09)**

How does the Information Technology Act, 2000 enable the authentication of records using digital signatures**?** **(Nov, 09)**

Authentication of electronic records in Information Technology (Amended) Act 2008. **(May, 11)**

Chapter- II of IT Act, 2000 gives legal recognition to electronic records and digital signatures. It contains only section 3.

[Section 3] **Authentication of Electronic Records:**

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation - For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Chapter-ii: Digital signature and electronic signature

Section 3: Authentication of Electronic records

Section 3A: Electronic Signature

Chapter-iii: Electronic governance

How does the Information Technology Act, 2000 enable the objective of the Government in spreading e-governance? **(Nov, 09)**

Chapter III is one of the most important chapters of IT Act 2000. It deals with the procedures to be followed for sending and

receiving of electronic records. This chapter contains sections 4 to 10.

Section 4 - This section provides for *legal recognition of electronic records.* **Section 5** - This section provides for *legal recognition of Digital Signatures.*

Section 6 - lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

Section 7 - This section provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained in the electronic form with the following conditions:

(i) the information therein remains accessible so as to be usable subsequently,

(ii) it is retained in its original format ,

(iii) the details such as origin, destination, dates and time of dispatch or receipt of such electronic record.

Section 8 - It provides for the publication of rules, regulations and notifications in the Electronic Gazette.

Sec. 4: Legal recognition of Electronic records.
Sec. 5: Legal recognition of Electronic signature.
Sec. 6: Use of electronic record and electronic signature in government and its agencies. **(RTP 14N)**
Sec. 7: Retention of electronic records. **(RTP-15M) (MT-15M).**
To retain their e-documents for specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology Act, 2000? **(May, 10)**
What is the provision given in Information Technology (Amended) Act 2008 for the retention of electronic records? **(May, 11)**
How is the term 'Electronic Record' defined in IT (Amended) Act 2008? What is the provision given in the IT Act for the retention of Electronic Records? **(May, 12)**
"Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

[Section 7] Retention of Electronic Records:

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, -
   (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
   (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

   the details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record: **However,**

   this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Publication of rules. regulation, etc. in Electronic Gazette.

Describe the provisions for retention of electronic records under Section 7 of Information Technology (Amendment) Act, 2008. (**May, 14)**
Sec. 7A: Audit of document in electronic form.
Sec. 8: Publication of rules, regulation, bye laws, notification in the Electronic Gazette.
Sec. 9: Section 6, 7 & 8 Not to confer Right to insist document should be accepted in electronic form.
Sec. 10: power to make rules by CG in respect of electronic signature.
Describe the power to make rules by Central Government in respect of Electronic Signature under Section 10 of Information Technology (Amended) Act 2008. **(May, 12)**
Section 10 gives the Central Government following powers to make rules in respect of Electronic Signature

(a) specify the type of Electronic Signature;
(b) specify how Electronic Signature shall be affixed and the format of the signatures;
(c) to identify the person who has affixed the Electronic Signature;
(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
(e) other matter which is necessary to give legal effect to Electronic Signature.

Sec 10A: Validity of contracts formed through electronic means.
Chapter V: **Secure** Electronic Records and **Secure** Electronic Signature;
Sec. 14: Conditions for deeming an electronic record as secure.
Sec. 15: Condition for deeming an electronic signature as secure.
Chapter IX: Penalties and Adjudication;
Sec. 43: Penalty and Compensation for damage of computer, computer system etc.
Sec. 44: Penalty for failure to furnish information, return to controller or CA.

Chapter XI: Offences under the IT Act
Sec. 65: Tampering with computer source code (extend up to 3 years or with fine upto ` 2 lakhs or both)
Sec. 66: Computer Related Offence (extend up to 3 years or with fine upto ` 5 lakhs or both)
Sec. 66A: Punishment for sending offensive messages through communication services etc.(2years & Fine) **(RTP-15M). (RTP 14N)**
As per the decision of Apex court dated 24th arch, 2015; Section 66A has been declared Unconstitutional as it is violative of Article 19(1)(a) related to freedom of speech and expressions. Now comments on social networking sites will not be offensive unless they come under the provisions of the Indian Panel Code, 1860.
Sec. 66B: Punishment for dishonestly receiving stolen computer resources or communication devices (extend up to 3 years or with fine upto ` 1 lakhs or with both) **(RTP-15M). (RTP 14N)**

Sec. 66C: Punishment for Identity theft (extend up to 3 years & also fine upto `1 lakh)
Sec. 66D: Punishment for cheating by personation by using computer resources (extend up to 3 years & also with fine upto ` 1 lakh)
Sec. 66E Punishment for violation of privacy (extend up to 3 years or with fine not exceeding ` 2 lakhs or both) **(RTP 14N)**
Sec. 66F: Punishment for cyber terrorism (Imprisonment which may extend to Imprisonment for life)
Sec. 67: Punishment for publishing or transmitting obscene material in electronic form (5years & `10 lakhs)
Sec. 67A: Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form (7 years and & also with a fine may extend to ` 10 lakhs)
Sec. 67B: Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form) (5 years and & also with a fine may extend to ` 10 lakhs)

Sec. 67C: Prevention and retention of information by intermediary (2years or to a fine 1 lakh ` or with both)
Sec. 68: Power of controller to give directions (3 years or to a fine 1 lakh ` or with both) **(RTP-15M).**
Sec. 69: Power to issue direction for interception or monitoring or decryption of any information through any computer resources (7 years and & also with a fine)
Sec. 69A: Power to issue direction for blocking for public access of any information through any computer resources (7 years and & also with a fine)
Sec. 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security (3years and & also with a fine)
Sec. 70: Protected system (10years and & also with a fine)
Sec. 70A: National Nodal agency
Sec. 70B: Indian computer emergency response team to serve as national agency for incident response
Sec. 71: Penalty for misrepresentation (2 year or a fine 1 lakh` or with both)
Sec. 72: Penalty for breach of confidentiality and privacy (2 year or a fine 1 lakh` or with both)
Sec. 72A: Punishment for disclosure of information in breach of lawful contract (3year or a fine 5 lakh` or with both)
Sec. 73: Penalty for publishing electronic signature certificate false in certain particulars(2 year or a fine 1 lakh` or with both)
Sec. 74: Publication for fraudulent purpose (2 year or a fine 1 lakh` or with both)
Sec. 75: Act to apply for offence or contravention committed outside India
Sec. 76: Confiscation

Chapter XII: Intermediary not to be liable in certain cases
Sec. 79: Exemption from liability of intermediary in certain cases

Chapter XIIA: Examiner of electronic evidence
Sec. 79A: CG to notify examiner of electronic evidence

Chapter XIII: Miscellaneous
Sec. 80: Power of police officer and other officer to Enter, search etc **(RTP-15M) (RTP 14N)**
Sec. 81: Act to have overriding effect

Sec. 81AC: Application of Act to electronic cheque and Truncated cheque
Sec. 84C: Punishment for attempt to commit offences
Sec. 85: Offences by Companies

State the liabilities of companies under section 85 of Information Technology Act, 2000. **(Nov, 08)**

Liability of Companies under Section 85 of Information Technology Act, 2000: Where a company commits any offence under this Act or any rule thereunder, every person who, at the time of the contravention, was in charge of and was responsible for the conduct of the business of the company shall be guilty of the contravention. However, he shall not be liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent the contravention.

Further, where a contravention has been committed by a company, and it is proved that the contravention took place with the connivance or consent of or due to any negligence on the part of any director, manager, secretary or other officer of the company, such officer shall be deemed to be guilty and shall be liable to be proceeded against and punished accordingly.

For the purposes of this section, 'company' includes a firm or other association of persons and 'director' in relation to a firm means a partner in the firm.

The Information Technology Act will go a long way in facilitating and regulating electronic commerce. It has provided a legal framework for smooth conduct of e-commerce. It has tackled the following legal issues associated with e-commerce:

Requirement of writing
Requirement of a document
Requirement of a signature and
Requirement of legal recognition for electronic messages,
Records and documents to be admitted in evidence in a court of law.

Requirement of various Authorities for System Controls and Audit:

In Indian scenario audit of system controls are mandatory requirement in the following cases:

1. **Requirement of IRDA for System Controls and Audit**
2. **Requirement of RBI for System Controls and Audit**
3. **Requirement of SEBI for System Controls and Audit**

Requirement of IRDA for System Controls and Audit
It focuses on compliance with laws and regulations, which are given as follows:

- **(i) System audit**
- **(ii) Preliminaries**
- **(iii) System controls**

Requirement of RBI for System Controls and Audit

- Auditor qualification such as CISA, DISA offered by ISACA, RBI has an Inspection Wing, Large Form Audit Report (LAFR) has specific question relating to IT areas.

Requirement of SEBI for System Controls and Audit

The manner of selecting auditors builds confidence among various stakeholders. Describe SEBI norms for selecting an auditor. **(May, 15)**

The SEBI norms for Auditor Selection are as follows:

- Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
- The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (ISC)².
- The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. He should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

ABC Ltd. is a security market intermediary, providing depository services. Briefly explain the **relevant requirements** with respect to annual systems audit mandated by SEBI in this regard. **(Nov, 14)**

(i) System Audit: Norms, Terms of reference
(ii) Audit Report Norms
(iii) Auditor selection Norms: 3 years experience, DISA, CISA qualification, familiarity threat.
(iv) System controls

Discuss the guidelines recommended by SEBI to conduct audit of system. RTP

Mandatory audits of systems and processes bring transparency in the complex workings of SEBI, prove integrity of the transactions and build confidence among the stakeholders, SEBI has manadated that exchanges shall conduct annual system audit by a reputed independent auditor. Guidelines are

- The audit shall be conducted according to the Norms, TOR, and Guidelines issued by SEBI.
- Stock exchange/depository (Auditee) may negotiate and the board of Stock Exchange/ Depository shall appoint the Auditor based on the prescribed Selection Norms and TOR. The auditor can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.
- The scope of the audit may be extended by SEBI, considering the changes which have taken place during last year or post previous audit report.
- Audit schedule shall be submitted to SEBI at least 2 months in advance, along with scope of current audit and previous audit.
- Audit has to be conducted and the audit report be submitted to the auditee. The report should have specific compliance/non-compliance issues, observations for minor deviations as well as qualitative comments for scope for improvement. The report should also take previous audit report in consideration and cover any open items therein.
- The auditee management provides their comments about the Non-Conformities and observations. For each NC, specific Time-bound (within 3 months) corrective action must be taken and reported to SEBI. The auditor should indicate if a follow-on audit is required to review status of NCs. The report along with management comments shall be submitted to SEBI within 1 month of completion of the audit. Sample areas of review covered by IS audit assignments are given there.

Cyber Forensic and Cyber Fraud Investigation

Cyber, means on 'The Net' that is online.

Forensic is a scientific method of investigation and analysis technique to gather, process, interpret, and to use evidence to provide **a conclusive** description of activities in a way that is suitable for presentation in **a court of law**.

Cyber Investigation is an investigation method gathering **digital evidence** to be produced in court of law. Court rulings and amendment to Cyber laws now permit courts **to rely upon digital evidence.**

Security Standards

National Cyber Security Policy, 2013.

Some of the most relevant and used standards and frameworks in the security space are given below.

(1) ISO 27001
(2) SA 402
(3) ITIL (IT infrastructure Library)

ISO 27001

Discuss briefly, the four phases of Information Security Management System (ISMS) prescribed by ISO 27001. **(Nov, 14) (MT-Nov, 14)**

Systematic approach for **managing** confidential or sensitive information.

Four phases of ISMS: it prescribes "how to manage information security through a system of information security management.

The four phases of Information Security Management System (ISMS) prescribed by ISO 27001 are as follows:

The Plan Phase – This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).

The Do Phase – This phase includes carrying out everything that was planned during the previous phase.

The Check Phase – The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.

The Act Phase – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep the ISMS effective.

SA 402
Audit consideration relating to an entity using service organisation

ITIL
It is a set of practices for IT services management that focuses on aligning IT services with the needs of business. It also brought a rationalization in the number of volumes included in the set, which now comprises the followings;

- Service strategy
- Service design
- Service transition
- Service operation and
- Continual service improvement

Mr. A has **received some information** about Mr. B on his cellphone. He knows that this information has been stolen by the sender. He not only retained this information but also sends it to Mr. B and his friends. Because of this act Mr. B is annoyed and his life is in danger.

Mr. B seeks your advice, under what sections of Information Technology (Amendment) Act, 2008, he can file an FIR with police? Advise Mr. B detailing the applicable sections of the Act. **(May, 13) (MT –Nov, 14)**

It is not clear whether Mr. B wants to file an FIR with police against Mr. A or sender, who has stolen his information or both.

Considering the most feasible assumption that if Mr. B wants to file an FIR against Mr. A then he may file the same under the following Section of Information Technology (Amendment) Act, 2008:

- Section 66 A: Punishment for sending offensive messages through communication service, etc.;
- Section 66 B: Punishment for dishonestly receiving stolen computer resource or communication device; and
- Section 66 E: Punishment for violation of privacy.

All these applicable sections in this case are given as follows:

[Section 66 A] Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,-

(a) any **information** that is grossly offensive or has menacing character; or

(c) any **information** which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently **by making** use of such computer resource or a communication device, any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: For the purposes of this section, terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

[Section 66 B] Punishment for dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

[Section 66E] Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

However, the answer may also be written considering the other two assumptions, accordingly.

Mr. A is regularly **sending obscene in electronic form** to Ms. B. When Ms. B made a complaint to Police, it was found that all the communications were sent through XYZ network service provider. Police have held both Mr. A and XYZ network service provider as liable for this act. Suggest under what provisions of Information Technology (Amendment) Act, 2008, the XYZ

network service provider can get exemption from the liability? Also discuss the relevant provisions of the above section. **(May, 14)**

As per Information Technology (Amendment) Act 2008, the XYZ network service provider can get exemption from the liability under provisions of sub-sections 1 and 2 of **Section 79: Exemption from liability of intermediary in certain cases**.

The relevant provisions of the above section are given as follows:

[Section 79] Exemption from liability of intermediary in certain cases:

1. Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.
2. The provisions of sub-section (1) shall apply if-
   (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
   (b) the intermediary does not-
      (i) initiate the transmission,
      (ii) select the receiver of the transmission, and
      (iii) select or modify the information contained in the transmission
   (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

Mr. A has hacked into Defence Information Systems with an intention to steal classified information that threatens the security and sovereignty of India. He has used the services of a local cafe, 'CyberNet' for this purpose. The owner of 'CyberNet' tries to stop Mr. A but is threatened by Mr. A. Hence the owner of 'CyberNet' does not disclose A's activities to anyone. Mr. A is caught by the Vigilance Officers of the department.

(i) Is Mr. A punishable for his activities?
(ii) Is the intermediary, 'CyberNet' liable?

Please discuss the liabilities enunciated under the relevant sections of the Information Technology Act, 2000 in the above two cases**. (May, 15)**

Solution: (i) Yes, Mr. A is punishable for his activities under the Section 66F.

[Section 66F(1)(B)] Punishment for cyber terrorism

Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

Considering the facts provided in the case where Mr. A hacked into Defense Information System with an intention to steal classified information threatening the security and sovereignty of India, Mr. A is punishable for his activities.

(ii)Yes, Intermediary 'CyberNet' is liable under the Section 79.

[Section 79] Exemption from liability of intermediary in certain cases

1. Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.
2. The provisions of sub-section (1) shall apply if -
   (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
   (b) the intermediary does not-
      (i) initiate the transmission,
      (ii) select the receiver of the transmission, and
      (iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

Thus, according to Section 79(2)(c); the Intermediary 'CyberNet' failed to observe due diligence in discharging his duties and also the other guidelines as prescribed by the Central Government. So, Intermediary 'CyberNet' is liable.

Chapter 8: Emerging Technologies

Cloud Computing (RTP-15M).

The word "The Cloud" is used as a metaphor for the "Internet" so the phrase "Cloud Computing" means "A Type of Internet Based Computing," where **different services**--- such as Servers, Storage and Applications--- are delivered to an organisation's computers and devices through the internet.

It simply means the use of computing resources **as a service** through the network, typically the internet. Cloud computing dedicates a song for service receiver: मैं जहाँ रहुँ, मैं कहीं भी हुँ, बस तेरी याद साथ है,

Pertinent Issues

Pertinent issue discuss some of the pertinent objectives in order to achieve the goals of Cloud computing.

- **Threshold policy**
- **Interoperability**
- **Hidden cost**
- **Unexpected behaviour**
- **Security issue**
- **Software development in cloud**
- **Environmental friendly cloud computing**

Goal of Cloud Computing

Discuss the goal of cloud computing. **(MT –Nov, 14)**

Discuss some of the pertinent objectives in order **to achieve the goals** of Cloud Computing. **(Nov, 14)**

Some of the pertinent objectives in order to achieve the goals of Cloud Computing are as follows:

→ To pool available resources together into a highly efficient infrastructure and whose cost are aligned with the what resources are actually used (सभी resources एक हीं platform पर available हौगां);
→ To access services and data from anywhere at any time;
→ To scale the IT ecosystem quickly, easily and cost effectively based on evolving business needs;
→ To consolidate IT infrastructure into a more integrated and manageable environment;
→ To reduce cost related to IT energy/power consumption;
→ To enable or improve "Anywhere Access" for ever increasing users; and
→ Needs based provision of service. **(RTP 14N)**

CC Architecture (CCA):

CCA of a CC is the structure, which comprise all the required hardware and software to support CC. A CCA consist of Front End architecture (FEA) and Back End Architecture (BEA).

- FEA: Client Devices or Computer Network and Applications
- BEA: Cloud itself, services **facilitating** peripherals.

CC Environment (CCE)

CCE can **consist** of multiple types of clouds based on **their deployment and usage**.

- **Public C**.: Used by general public, managed by 3rd part over the internet, pay-per-use basis, model is SaaS. Advantages. Also called Provider Cloud. **(RTP 14N)**
- **Private C.** : Used execlusively by an orgn and reside within the Orgn, built by IT department within the Orgn.
- **Hybrid C**. : Combination of above.

CC **Models:** Services are based on several fundamental models- (IPS बनेगा Nilesh Curve)

1. Infrastructure as a service(IaaS): Offer computer (virtual machine) and other resources as service.
2. Platform as a service(PaaS): offer computing platform including OS, P. Language execution environment, and database and web server. **(RTP-15M).**
3. Software as a service (SaaS): provides access large variety of applications over the internet typically hosted in the provider infrastructure. **(RTP-15M).**
4. Network as a service (NaaS): Use network/transport connecting services.
5. Communication as a service (CaaS):

Characteristic of CC (SAHi2 **पनीर और** PVM, Mutton, Sack)

- **High scalability:** Cloud environments enable **servicing of business requirements for larger audiences**, through high scalability.

- **Agility:** The cloud works in the **'distributed mode 'environment**. It **shares** resources **among users and tasks**, while improving efficiency and agility (responsiveness).
- **High Availability and Reliability:** Availability of servers is **supposed to be high and more reliable** as the chances of infrastructure failure are minimal.
- **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
- **Services in pay-per-use basis:** SLAs between the provider and the user must be defined when offering services in pay per use mode
- **Performance:** It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Virtualisation:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- **Maintenance:** The cloud computing applications are easier, because they are not to be installed on each user's computer and can be accessed from different places.

Advantages of CC

What are the advantages of cloud computing environment? **(Nov, 15)** (CA & BA Easy & Quickly **से पास हो जाता है**) **(MT, Nov, 14)**

- **Cost efficiency**: Cloud computing is probably the most cost efficient method **to use, maintain and upgrade**. The cloud is available **at much cheaper rates** and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, **which make it very reasonable for the company**.
- **Almost unlimited storage**: Storing information in the cloud **gives us almost unlimited storage capacity**.
- **Backup & recovery**: Since all the data is stored in the cloud, **backing it up and restoring the same is relatively much easier than storing the same on a physical device.**
- **Automatic software integration**: In the cloud, software integration is usually something that **occurs automatically**. This means that we do **not need to take additional efforts to customize and integrate** the applications as per our preferences.
- **Easy access to information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection.
- **Quick development**: Lastly and most importantly, cloud computing **gives us the advantage of quick deployment**. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes.

Challenges of CC(CIA & GAAPI, DISA से Tuli Lounge मे मीलने गएं है)(QPM) (RTP 14N)

Management wants to know the major challenges in using Cloud Computing technology for running the new web application. Write any five challenges. **(May, 15)**

→ **C: Confidentiality: Prevention of unauthorised disclosure of information is referred to as c.**
→ **I: Integrity**
→ **A: Availability**
→ **G: Governance**
→ **A: Audit**
→ **A: Architecture**
→ **P: Privacy**
→ **I: Identity management and access control**
→ **D: Data stealing**
→ **I: Incident Response**
→ **S: Software Location**
→ **A: Application security**
→ **T: Trust**
→ **L: Legal Issues and compliance**

Mobile Computing (MT- Nov, 14)

It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link.

MC services

MC Benefits

But, more specifically, it leads to a range of tangible benefits, including the following:

© It provides mobile workforce **with remote access** to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.

- © It enables mobile sales personnel to **update work order status in real-time**, facilitating excellent communication.
- © It **facilitates** access to corporate services and information **at any time, from anywhere**.
- © It provides **remote access to the corporate Knowledgebase** at the job location.
- © It enables to **improve management effectiveness** by enhancing information quality, information flow, and ability to control a mobile workforce.

BYOD (Bring Your Own Device)

BYOD (Bring Your Own Device) refers to business policy **that allows employees to use their preferred computing devices**, like smart phones and laptops for business purposes. It means **employees are welcome to use personal devices** (laptops, smart phones, tablets etc.) **to connect to the corporate network** to access information and application.

Emerging BYOD threats

If employee of the company are allowed to use personal devices such as laptop, Smartphone, tablets etc. To connect and access the data what would be security risk involved? Classify and elaborate such risk. **(Nov, 15)**

(BYOD से NADI मे बाढ आने का threats है)

- **N: Network Risk:** It is normally exemplified and hidden in 'Lack of Device Visibility'.
- **A: Application Risk:** It is normally exemplified and hidden in **'**Application Viruses and Malware'.
- **D: Device Risk:** It is normally exemplified and hidden in 'Loss of Devices'.
- **I: Implementation Risk:** It is normally exemplified and hidden in 'Weak BYOD Policy'.

Social Media and Related Aspects

Web 1.0: With this we can only read/see web page content but with web 2.0 we can write as well e.g. Face Book.

Web 2.0 (2nd generation) basically refers to the transition from static HTML web pages **to more dynamic** web that is more organised and is based on serving web application to users.

Components of web 2.0 for social network (WiCo FiFo BedMinton)

Wikis: A Wiki is a **set of co-related pages** on a particular subject and **allow users to share content**. Wikis **replace** the complex document management systems and **are very easy to create and maintain**.

Communities: These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are a number of tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.

File Sharing: This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.

Folksonomy: Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.

Blogging: Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics

Mashups: This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service.

Green IT

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

Green computing is the environmentally responsible use of computers and related resources. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste). One of the earliest initiatives toward green computing in the United States was the voluntary labeling program known as Energy Star.

Major steps, which can be followed for green IT, are given as follows **(RTP 14N)**

Best practices of Green IT **(May, 15)**

What do you understand by Green It? Steps **(MT,15M)**

What are your recommendations for efficient use of computer & IT resources to achieve the objectives of "**Green computing**"? **(Nov, 14) (PM)**

Some of the recommendation for efficient use of computer & IT resources to achieve the objectives of "**Green computing** are as follows:

Some of such steps for Green IT include the following:

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