FINAL COURSE

PRACTICE MANUAL

PAPER : 6

INFORMATION SYSTEMS CONTROL AND AUDIT

BOARD OF STUDIES
THE INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA

This Practice Manual has been prepared by the faculty of the Board of Studies. The objective of the Practice Manual is to provide teaching material to the students to enable them to obtain knowledge and skills in the subject. In case students need any clarifications or have any suggestions to make for further improvement of the material contained herein, they may write to the Director of Studies.

All care has been taken to provide interpretations and discussions in a manner useful for the students. However, the Practice Manual has not been specifically discussed by the Council of the Institute or any of its Committees and the views expressed herein may not be taken to necessarily represent the views of the Council or any of its Committees.

Permission of the Institute is essential for reproduction of any portion of this material.

Revised Edition	:	January, 2016
Website	:	www.icai.org
E-mail	:	bosnoida@icai.org
Committee / Department	:	Board of Studies
ISBN No.	:	978-81-8441-362-5
Price	:	₹ 100
Published by	:	The Publication Department on behalf of The Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi – 110 002.
Printed by	:	Repro India Ltd. December/2015/P1869 (Revised)

A WORD ABOUT PRACTICE MANUAL

Dependency on Information Technology (IT) enabled services is increasing at a very fast rate in the current highly connected world. Traditional working setups have been replaced by the technology driven frameworks and networks. The flexibility of the software systems has transformed the success stories of the organizations' mission, plans, and policies. Accordingly, accounting professionals also interact with computer-based information systems on a regular basis. As primary users of information systems in organizations, accountants need to participate in the design, development and operations of IT systems. In addition, they need to measure and evaluate the performance of information systems with the help of appropriate controls. Internal and external auditors must assess the quality of information systems and evaluate the accuracy of information input and output. Hence, Chartered Accountants must have the conceptual clarity to deal with different controls adapted in these systems and other important tasks.

In today's dynamic and changing economic environment, businesses are subjected to greater risks than ever before. Accordingly, auditors should also be in a position to identify the business risks that an organization can face and the risk management policies that an organization has to adapt to effectively manage those risks and particularly for Information Systems and their security. There are a number of Chartered Accountants, who work as IS Auditors in their professional lifes in the environment of information systems. In addition, some of them work as IT Managers, responsible for the development of application systems, starting from the requirements analysis and till system maintenance.

For all these tasks, CAs require a thorough knowledge/understanding of the concepts of IT and accordingly, the Chartered Accountancy course has also included IT as a part of the course curriculum both at Intermediate (IPC) and Final levels. A paper on Information Systems Control and Audit forming a part of the final course helps the students to develop competencies and skill-sets in evaluation of controls and relevant evidence gathering in an IT environment using IT tools and techniques for effective and efficient performance of accounting, assurance and compliance services provided by a Chartered Accountant. The basic knowledge about IT gained at Intermediate (IPC) level is sought to be built up further through this paper.

Due to fast changing world of Information and Communication Technologies, the Institute felt an urgent need to relook the syllabus of IT related papers separately and hence, the syllabus of 'Information Systems Control and Audit' has been revised with a view to rationalize the same in the light of recent technological developments by making necessary additions/deletions and modifications therein.

This Practice Manual has been designed with the need of home-study and keeping distance-learning students in view. Such students require full coverage of the syllabus topics, and also the facility to undertake extensive questions' practice. The main aim of this Practice Manual is to provide guidance as to the manner of writing an answer in the examination. The main features of this Practice Manual are given as follows:

- **Concepts in Brief:** Important definitions, concepts and points have been given before each topic for quick recapitulation.
- **Questions:** Questions have been given in the same order in which the topics have been covered in the Study Material. Students are expected to attempt the questions and then compare their answers with the answers provided in the manual. In this way, they will be able to know the gaps in between and can improve their way of writing the answers in the examination.
- **Exercise:** Exercises have been given at the end of each chapter for independent practice.

In case you need any further clarification/guidance, please send your queries at bosnoida@icai.in/sukriti.arora@icai.in.

Happy Reading and Best Wishes!

Paper – 6: Information Systems Control and Audit

Statement indicating Chapter-wise distribution of Examination Questions along with Marks

Syllabus contents		**Syllabus covered in the examination held in**					
		November 2014		**May 2015**		**Total Marks**	**Avg. Marks**
Chapter No.	**Name of the Chapter**	**Questions**	**Marks**	**Questions**	**Marks**		
1	Concepts of Governance and Management of Information Systems	3(c), 4(b), 7(b), 7(c)	**18**	5(b), 6(a), 7(a), 7(e)	**20**	38	19
2	Information System Concepts	3(a), 5(b), 7(a)	**16**	3(b), 6(c)	**10**	26	13
3	Protection of Information Systems	3(b), 4(a), 5(c),	**16**	2(b), 4(a), 6(b)	**18**	34	17
4	Business Continuity Planning and Disaster Recovery Planning	5(a), 6(c), 7(d)	**14**	2(c), 7(c)	**8**	22	11
5	Acquisition, Development and Implementation of information Systems	6(b), 7(e)	**10**	3(a), 4(c)	**10**	20	10
6	Auditing of Information Systems	2(c), 6(a)	**10**	2(a), 4(b), 5(c), 7(b)	**20**	30	15
7	Information technology Regulatory Issues	2(a), 4(c)	**10**	3(c), 5(a)	**10**	20	10

8	Emerging Technologies	2(b)	**6**	7(d)	**4**	10	5
9	Questions based on Case - Studies	1(a), 1(b), 1(c), 1(d)	**20**	1(a), 1(b) 1(c), 1(d)	**20**	40	20

Note: Question paper of the aforementioned examination can be accessed from the 'BoS Knowledge Portal' under the section 'Students' on the Institute's website, www.icai.org.

CONTENTS

1

Concepts of Governance and Management of Information Systems

Basic Concepts

1. Key Concepts of Governance: Major terms used in governance are explained as follows:

- **Governance:** A **Governance** system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives.
- **Enterprise Governance: Enterprise Governance** can be defined as 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 appropriately and verifying that the organization's resources are used responsibly.

2. Enterprise Governance Dimensions: Enterprise Governance has two dimensions**:**

- **Corporate Governance or Conformance: Corporate Governance** is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The conformance dimension of governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.
- **Business Governance or Performance:** The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them.

3. IT Governance: The objective of IT governance is to determine and cause the desired behavior and results to achieve the strategic impact of IT. IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT activities to ensure effectiveness, accountability and compliance of IT.

4. Governance of Enterprise IT (GEIT): GEIT is a sub-set of corporate governance and facilitates implementation of a framework of relevant IS control within an enterprise and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Key Governance Practices of GEIT: The key governance practices of GEIT are - Evaluate the Governance System of Enterprise IT, Direct the Governance System, and Monitor the Governance System.

5. Corporate Governance, Enterprise Risk Management and Internal Controls: Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs.

Enterprise Risk Management (ERM) is a process, affected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The SEC's final rules define "Internal control over Financial Reporting" as a "process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company;
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements."

6. **Internal Controls as per Committee of Sponsoring Organizations (COSO):** According to COSO, Internal Control is comprised of five interrelated components: **Control Environment, Risk Assessment, Control Activities, Information and Communication,** and **Monitoring**.

7. **Role of IT in Enterprises:** It is needless to emphasize that IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

8. **IT Steering Committee:** Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

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

- **Strategic Planning:** In the context of Information systems, strategic planning refers to the planning undertaken by top management towards meeting long-term objectives of the enterprise. IT strategic plans provide direction to deployment of information systems and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation.
- **Management Control:** Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise.
- **Operational Control:** Operational control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

10. **Objective of IT Strategy:** The primary objective of IT strategy is to provide a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives.

11. **Classification of strategic Planning:** IT Strategy planning in an enterprise could be broadly classified into the following categories:

- Enterprise Strategic Plan,
- Information Systems Strategic Plan,
- Information Systems Requirements Plan, and
- Information Systems Applications and Facilities Plan.

12. Key Management Practices for Aligning IT Strategy with Enterprise Strategy: The key management practices, which are required for aligning IT strategy with enterprise strategy are to understand enterprise direction, assess the current environment, capabilities and performance, define the target IT capabilities, conduct a gap analysis, define the strategic plan and road map and communicate the IT strategy and direction.

13. Business Value from use of IT: Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost.

The key management practices, which need to be implemented for evaluating 'whether business value is derived from IT', are highlighted as under: Evaluate Value Optimization, Direct Value Optimization and Monitor Value Optimization.

14. Risk Management: Risk is the possibility of something adverse happening, resulting in potential loss/exposure. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources.

15. Related Terms: Various terminologies relating to risk management are given as follows:

Asset: Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees.

It is the purpose of Information Security Personnel to identify the threats against the assets, the risks and the associated potential damage to, and the safeguarding of Information Assets.

Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

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

Exposure: An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example; loss of business, failure to perform the system's mission, loss of reputation, violation of privacy and loss of resources etc.

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

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

Risk: Formally, Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset, **Risk Analysis** is defined as the process of identifying security risks and determining their magnitude and impact on an organization. **Risk assessment** includes the following:

- Identification of threats and vulnerabilities in the system;
- Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and
- The identification and analysis of security controls for the information system.

Countermeasure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as countermeasure. For example, well known threat 'spoofing the user identity', has two countermeasures:

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

The relationship and different activities among these aforementioned terms may be understood by the following Fig. 1.1:

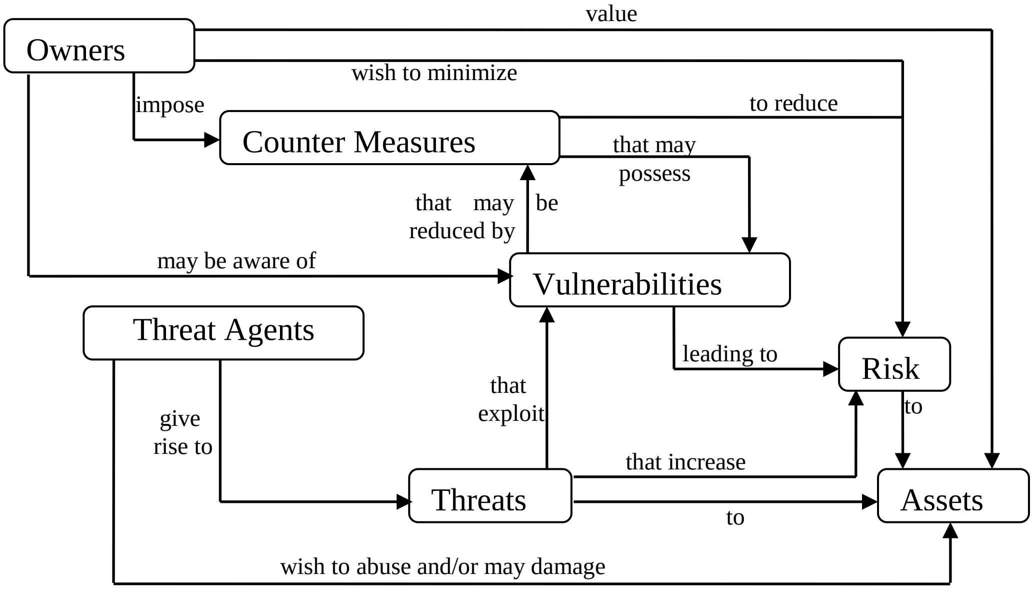


Fig. 1.1: Risk and Related Terms[*]

16. Risk Management Strategies: Major risk management strategies are Tolerate/Accept the risk, Terminate/Eliminate the risk, Transfer/Share the risk, Treat/ mitigate the risk and Turn back.

[*] Source: http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF p.14

17. Key Governance Practices of Risk Management: The key governance practices for evaluating risk management is to evaluate risk management, direct risk management and monitor risk management.

18. Key Management Practices of Risk Management: Key Management Practices for implementing Risk Management: Collect Data, Analyze Risk, Maintain a Risk Profile, Articulate Risk, Define a Risk Management Action Portfolio and Respond to Risk.

19. Metrics of Risk Management: Some of the key metrics are as follows:

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk Assessment;
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

20. COBIT 5 - A GEIT Framework: COBIT 5 helps enterprises to manage IT related risk and ensures 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.

21. Components in COBIT: The components of COBIT are Framework, Process Descriptions, Control Objectives, Management Guidelines, and Maturity Models.

22. Five Principles of COBIT 5: These principles are shown in Fig. 1.2:

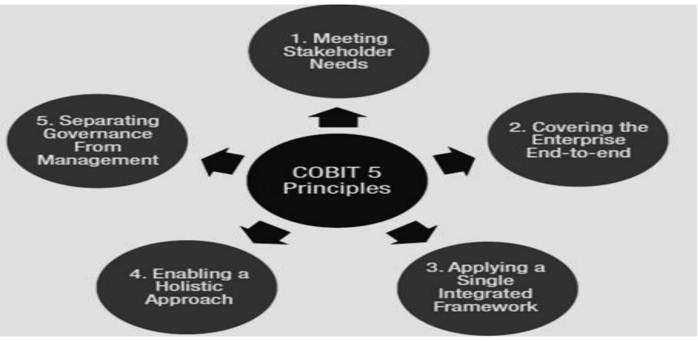

1. Meeting Stakeholder Needs
5. Separating Governance From Management
COBIT 5 Principles
2. Covering the Enterprise End-to-end
4. Enabling a Holistic Approach
3. Applying a Single Integrated Framework

Fig. 1.2: Five Principles of COBIT 5[*]

23. COBIT 5 Process Reference Model: COBIT 5 includes a Process Reference Model, which defines and describes in detail a number of governance and management processes of enterprise

[*] Source: www.isaca.org

IT into two main process domains- **Governance** and **Management** as shown in Fig. 1.3. It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers.

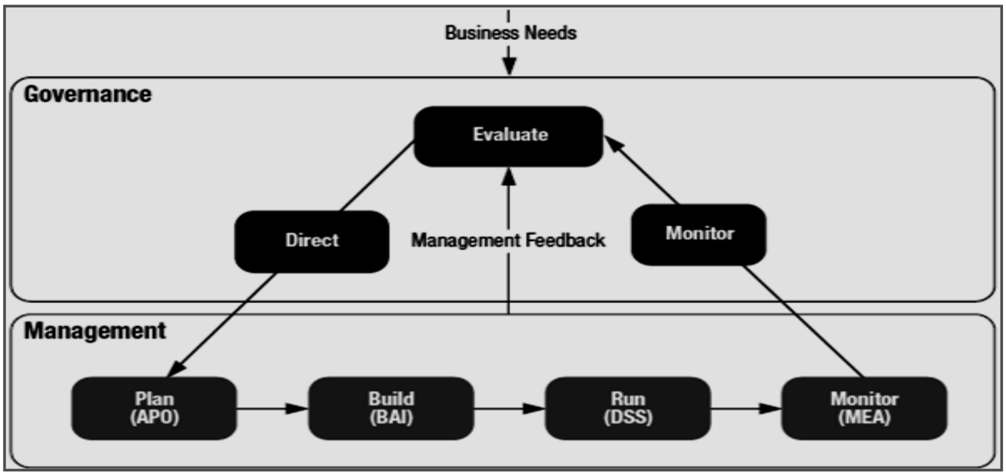


Fig. 1.3: Key Areas of Governance and Management∗

24. Seven Enablers of COBIT 5: The COBIT 5 framework describes seven categories of enablers, which are shown in Fig. 1.4:

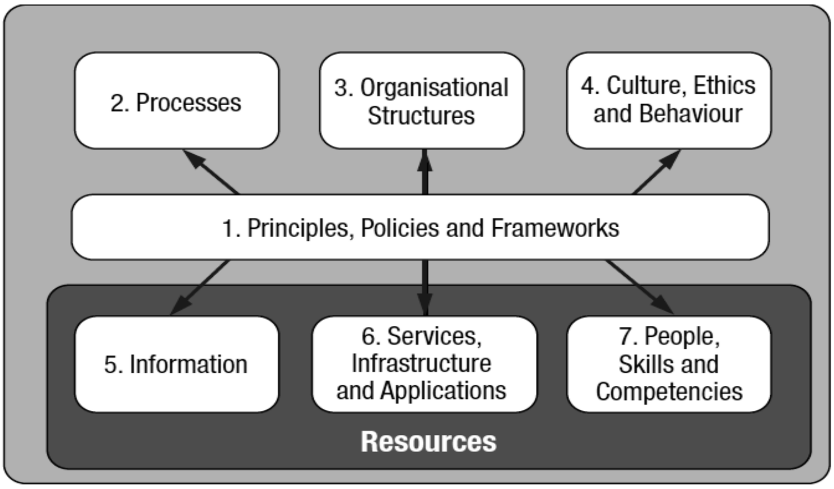

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Fig. 1.4: Seven Enablers of COBIT 5[*]

25. Risk Management in COBIT 5: A pictorial representation of various activities relating to risk management is given in Fig. 1.5:

[*] Source: www.isaca.org

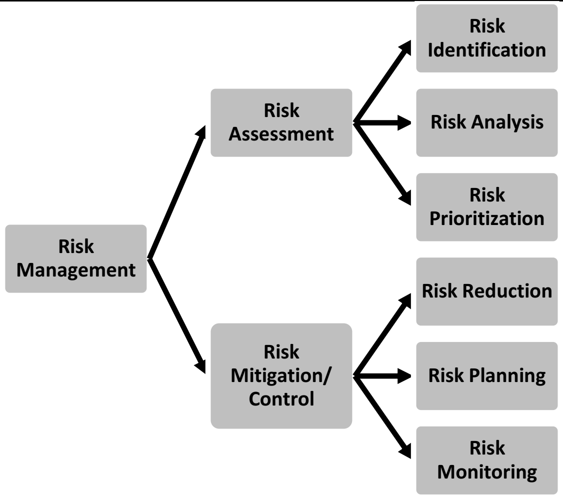


Fig. 1.5: Risk Management

26. Key Management Practices of IT Compliance: COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. The practices are: Identify External Compliance Requirements, Optimize Response to External Requirements, Conform External Compliance and Obtain Assurance of External Compliance.

27. Using COBIT 5 for Information System Assurance: The Fig. 1.6 provide sample examples of the different assurance needs, which can be performed by using COBIT 5.

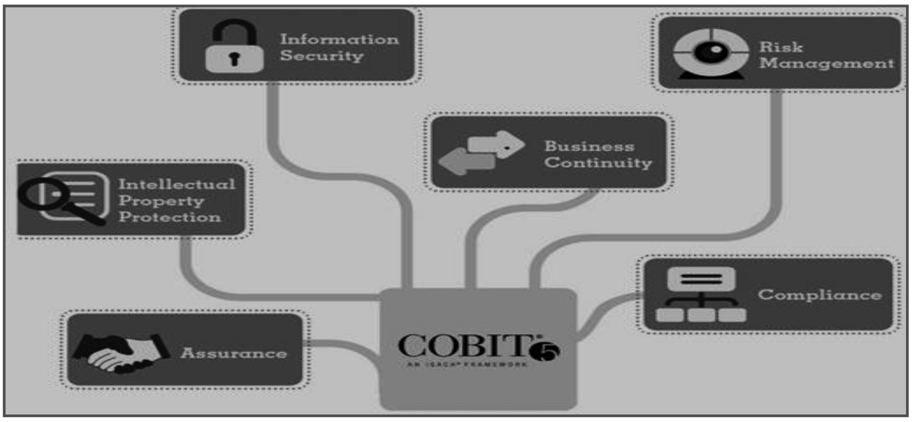


Fig. 1.6: Assurance Needs of COBIT 5*

28. Sample Areas of GRC for Review by Internal Auditors: Major areas, which can be reviewed by internal auditors as part of review of Governance, Risk and Compliance are given

* Source: www..isaca.org

as follows:

- **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process.
- **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities.
- **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
- **Interpretation:** Determining whether risk management processes are effective based on the internal auditor's assessment.
- **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.
- **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems.
- **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
- **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

29. Sample Areas of Review of Assessing and Managing Risks: This review broadly considers whether the enterprise is engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks. The specific areas evaluated are:

- Risk management ownership and accountability;
- Different kinds of IT risks (technology, security, continuity, regulatory, etc.);
- Defined and communicated risk tolerance profile;
- Root cause analyses and risk mitigation measures;
- Quantitative and/or qualitative risk measurement;

- Risk assessment methodology; and
- Risk action plan and Timely reassessment.

30. Evaluating and Assessing the System of Internal Controls: The key management practices for assessing and evaluating the system of internal controls in an enterprise are: Monitor Internal Controls, Review Business Process Controls Effectiveness, Perform Control Self-assessments, Identify and Report Control Deficiencies, Ensure that assurance providers are independent and qualified, Plan Assurance Initiatives, Scope assurance initiatives and Execute assurance initiatives.

Question 1

Explain the key benefits of IT Governance achieved at highest level in an organization.

Answer

The benefits, which are achieved by implementing/improving governance or management of enterprise IT, would depend on the specific and unique environment of every enterprise. At the highest level, these could include:

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

Question 2

Write short notes on the following with reference to Governance Dimensions:

(i) Conformance or Corporate Governance Dimension

(ii) Performance or Business Governance Dimension

Answer

(i) Conformance or Corporate Governance Dimension: Corporate Governance is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. Corporate governance refers to the structures and processes for the direction and control of companies. Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders. The corporate governance provides a historic view and focuses on regulatory requirements. This covers corporate governance issues such as: Roles of the chairman and CEO, Role and composition of the board of directors, Board committees, Controls assurance and Risk management for compliance.

Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital. It is about doing good business to protect shareholders' interest. Corporate Governance drives the corporate information needs to meet business objectives.

(ii) Performance or Business Governance Dimension: The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers. This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them. It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required.

The conformance dimension is monitored by the audit committee. However, the performance dimension in terms of the overall strategy is the responsibility of the full board but there is no dedicated oversight mechanism as comparable to the audit committee. Remuneration and financial reporting are scrutinized by a specialist board committee of independent non-executive directors and referred back to the full board. In contrast, the critical area of strategy does not get the same dedicated attention. There is thus an oversight gap in respect of strategy. One of the ways of dealing with this lacuna is to establish a strategy committee with status similar to other board committees and which will report to the board.

Question 3

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

Answer

Governance of Enterprise IT (GEIT): Governance of Enterprise IT is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.

Major benefits of GEIT are given as follows:

- It provides a 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 requirements.
- It ensures that the governance requirements for board members are met.

Question 4

Explain the key functions of IT Steering Committee in brief.

Answer

The key functions of the IT Steering Committee would include the following:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review 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 Board of Directors on IT activities on a regular basis.

Question 5

Discuss the key management practices, which are required for aligning IT strategy with enterprise strategy.

Answer

The key management practices, which are required for aligning IT strategy with enterprise strategy, are given as follows:

- **Understand enterprise direction:** Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).

- **Assess the current environment, capabilities and performance:** Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.
- **Define the target IT capabilities:** Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
- **Conduct a gap analysis:** Identify the gaps between the current and target environments and consider the alignment of assets (the capabilities that support services) with business outcomes to optimize investment in and utilization of the internal and external asset base. Consider the critical success factors to support strategy execution.
- **Define the strategic plan and road map:** Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals. Include how IT will support IT-enabled investment programs, business processes, IT services and IT assets. IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high-level road map.
- **Communicate the IT strategy and direction:** Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

The success of alignment of IT and business strategy can be measured by reviewing the percentage of enterprise strategic goals and requirements supported by IT strategic goals, extent of stakeholder satisfaction with scope of the planned portfolio of programs and services and the percentage of IT value drivers, which are mapped to business value drivers.

Question 6

'The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and how transparency of IT costs, benefits and risk is implemented'. Explain some of the key metrics, which can be used for such evaluation.

Answer

The key metrics, which can be used for such evaluation, are given as follows:

- Percentage of IT enabled investments where benefit realization is monitored through full economic life cycle;

- Percentage of IT services where expected benefits have been realized;
- Percentage of IT enabled investments where claimed benefits are met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

Question 7

Write short note on the following:

(i) Risk

(ii) Threat

(iii) Exposure

(iv) Attack

(v) Internal Controls as per COSO

(vi) Principles of COBIT 5

(vii) Vulnerability

(viii) Likelihood of threat

(ix) Countermeasure

(x) Residual Risk

Answer

(i) Risk: Formally, risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset.

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

(iii) Exposure: It is the extent of loss the organization has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example, loss of business, failure to perform the system's mission, loss of reputation, violation of privacy, loss of resources.

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

(v) 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.

(vi) The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective Governance and Management framework that optimizes information and technology investment and use for the benefit of stakeholders.

- **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.

(vii) Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats and can be exploited by the attackers. The weakness may be in information system/s, cryptographic systems or other components e.g. system security procedures, hardware design, internal controls that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system.

Some examples of vulnerabilities are as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors.
- Short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

In other words, Vulnerability is a state in a computing system (or set of systems), which must have at least one condition, out of the following:

- 'Allows an attacker to execute commands as another user' or
- 'Allows an attacker to access data that is contrary to the specified access restrictions for that data' or
- 'Allows an attacker to pose as another entity' or
- 'Allows an attacker to conduct a denial of service'.

(viii) Likelihood of threat: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

(ix) Countermeasure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system to a threat is referred as countermeasure. For example, the well known threat 'spoofing the user identity', has two countermeasures:

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

Similarly, for other vulnerabilities, different countermeasures may be used.

(x) Residual Risk: Any risk still remaining after the counter measures are analyzed and implemented is called Residual Risk. Residual risk must be kept at a minimal, acceptable level. As long as it is kept at an acceptable level, (i.e. the likelihood of the event occurring or the severity of the consequence is sufficiently reduced) the risk has been managed.

Question 8

Briefly explain various risk management strategies.

Answer

Risk Management Strategies: When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Various risk management strategies are explained as follows:

- **Tolerate/Accept the risk**. One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk**. It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk.** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.
- **Treat/mitigate the risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

Question 9

Describe key management practices for implementing risk management.

Answer

Key Management Practices for implementing Risk Management are given as follows:

- **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.
- **Analyze Risk:** Develop useful information to support risk decisions that take into account the business relevance of risk factors.

- **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes, including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.
- **Articulate Risk**: Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.
- **Respond to Risk**: Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

Question 10

Discuss various categories of enablers under COBIT 5.

Answer

Enablers are factors that, individually and collectively, influence whether something will work— in this case, governance and management of enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers (as shown in Fig. 1.4 in the 'Basic Concepts'):

1. Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
2. 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.
3. Organizational structures are the key decision-making entities in an enterprise.
4. Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.
5. 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.
6. Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
7. Skills and competencies are linked to people and are required for successful completion of all activities for making correct decisions and taking corrective actions.

Question 11

Discuss the areas, which should be reviewed by internal auditors as a part of the review of Governance, Risk and Compliance.

Answer

Major areas, which should be reviewed by internal auditors as a part of the review of Governance, Risk and Compliance, are given as follows:

- **Scope:** The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.
- **Governance:** The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:
  - Promoting appropriate ethics and values within the organization;
  - Ensuring effective organizational performance management and accountability;
  - Communicating risk and control information to appropriate areas of the organization; and
  - Coordinating the activities of and communicating information among the board, external and internal auditors, and management.
- **Evaluate Enterprise Ethics:** The internal audit activity must evaluate the design, implementation and effectiveness of the organization's ethics related objectives, programs and activities. The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.
- **Risk Management:** The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.
- **Interpretation:** Determining whether risk management processes are effective in a judgment resulting from the internal auditor's assessment that:
  - Organizational objectives support and align with the organization's mission;
  - Significant risks are identified and assessed;
  - Appropriate risk responses are selected that align risks with the organization's risk appetite; and
  - Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

- **Risk Management Process:** The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness. Risk management processes are monitored through on-going management activities, separate evaluations, or both.
- **Evaluate Risk Exposures:** The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:
  - achievement of the organization's strategic objectives;
  - reliability and integrity of financial and operational information;
  - effectiveness and efficiency of operations and programs;
  - safeguarding of assets; and
  - compliance with laws, regulations, policies, procedures, and contracts.
- **Evaluate Fraud and Fraud Risk:** The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.
- **Address Adequacy of Risk Management Process:** During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks. Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes. When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

Question 12

Discuss the key management practices for assessing and evaluating the system of internal controls in an enterprise in detail.

Answer

The key management practices for assessing and evaluating the system of internal controls in an enterprise are given as follows:

- **Monitor Internal Controls:** Continuously monitor, benchmark and improve the control environment and control framework to meet organizational objectives.
- **Review Business Process Controls Effectiveness:** Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centres, and network operations centres. This provides the business with the assurance

of control effectiveness to meet requirements related to business, regulatory and social responsibilities.

- **Perform Control Self-assessments:** Encourage management and process owners to take positive ownership of control improvement through a continuing program of self-assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.
- **Identify and Report Control Deficiencies:** Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.
- **Ensure that assurance providers are independent and qualified:** Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards
- **Plan Assurance Initiatives:** Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.
- **Scope assurance initiatives:** Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.
- **Execute assurance initiatives:** Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

Question 13

What do you understand by IT Governance? Write any three benefits of IT Governance.

Answer

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

Benefits of IT Governance

- ***Increased value delivered through enterprise IT;***
- ***Increased user satisfaction with IT services;***
- ***Improved agility in supporting business needs;***
- ***Better cost performance of IT;***
- ***Improved management and mitigation of IT-related business risk;***
- ***IT becoming an enabler for change rather than an inhibitor;***

- *Improved transparency and understanding of IT's contribution to the business;*
- *Improved compliance with relevant laws, regulations and policies; and*
- *More optimal utilization of IT resources.*

Question 14

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?

Answer

The key management practices complying with COBIT 5 for assessing and evaluating the system of IT internal controls in an enterprise are given as follows:

- *Monitor Internal Controls: Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.*
- *Review Business Process Controls Effectiveness: Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls, continuous controls monitoring, independent assessments, command and control centers, and network operations centers.*
- *Perform Control Self-assessments: Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.*
- *Identify and Report Control Deficiencies: Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.*
- *Ensure that assurance providers are independent and qualified: Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.*
- *Plan Assurance Initiatives: Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise.*
- *Scope assurance initiatives: Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.*

- *Execute assurance initiatives: Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.*

Question 15

The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective.

Answer

The key Management Practices for implementing IT Risk Management are given as follows:

- *Collect Data: To enable effective IT related risk identification, analysis and reporting.*
- *Analyze Risk: To develop useful information to support risk decisions.*
- *Maintain a Risk Profile: To maintain an inventory of known risks and risk attributes.*
- *Articulate Risk: To inform IT- related exposures and opportunities to all required stakeholders for appropriate response.*
- *Define a Risk Management Action Portfolio: To manage opportunities and reduce risk to an acceptable level as a portfolio.*
- *Respond to Risk: To respond limit the magnitude of loss from IT related events in a timely manner.*

Question 16

Discuss key management practices required for aligning IT Strategy with Enterprise Strategy.

Answer

The key management practices, which are required for aligning IT strategy with enterprise Strategy is as follows:

- *Understand enterprise direction: 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.**

Exercise

1. *Describe the major benefits achieved through proper governance in an organization.*
2. *What are the key governance practices that are required to implement GEIT in an enterprise?*
3. *Discuss key management practices, which are needed to be implemented for evaluating 'whether business value is derived from IT' in an organization.*
4. *'COBIT 5 provides various management practices for ensuring compliance with external compliances as relevant to the enterprise'. Explain these practices in brief.*
5. *Discuss some of the sample metrics for reviewing the process of evaluating and assessing compliance with external laws & regulations and IT compliances with internal policies.*
6. *Write short notes on the following:*

   (i) Role of IT in enterprises

   (ii) Integrating COBIT 5 with other frameworks

   (iii) Sample areas of review for assessing and managing risks

   (iv) Evaluating IT Governance Structure and Practices by Internal Auditors.

   (v) Components of COBIT 5.

   (vi) Benefits of COBIT 5.

2

Information Systems Concepts

Basic Concepts

1. **System:** A system is a group of inter connected components working towards the accomplishment of a common goal by accepting inputs and producing outputs in an ordered transformation process.

2. **Classification of Systems:** System can be classified on the basis of various parameters like elements, interactive behaviour, degree of human intervention and working output as shown in Fig. 2.1.

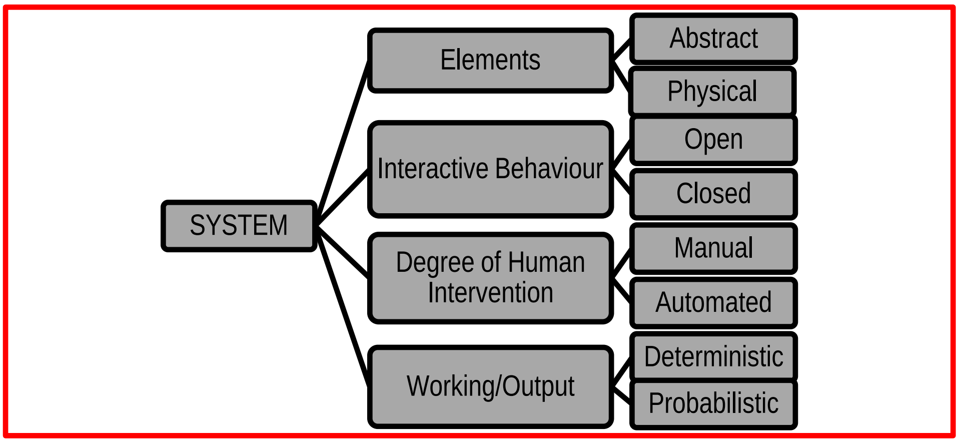


Fig. 2.1: Classification of System

2.1 **On the basis of Elements: Abstract System** also known as **Conceptual System or Model** can be defined as an orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about God and the relationship of humans to God. On the other hand, **Physical system** is a set of tangible elements, which operated together to accomplish an objective e.g. Computer system, University system etc.

2.2 **On the basis of Interactive behavior:** An **Open system** interacts with other systems in its environment whereas a **Closed system** does not interact with the environment and does not change with changes in environment. For example; Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of a number of components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation.

2.3 On the basis of degree of Human intervention: In a Manual System the data collection, maintenance and final reporting is done by human whereas it is carried out by computer system or say machine itself in the case of automated system.

2.4 On the basis of Working/Output: A Deterministic System operates in a predictable manner whereas Probabilistic System can be defined in terms of probable behaviour. For example; software that performs on a set of instructions is a deterministic system whereas inventory system is a probabilistic system where the average demand, average time for replenishment, etc. may be defined, but the exact value at any given time is not known.

3. Information Systems and its Components: With the help of Information Systems, enterprises and individuals are able to use computers to collect, store, process, analyze, and distribute information. An information system comprises people, hardware, software, data and network for communication support as shown in Fig. 2.2.

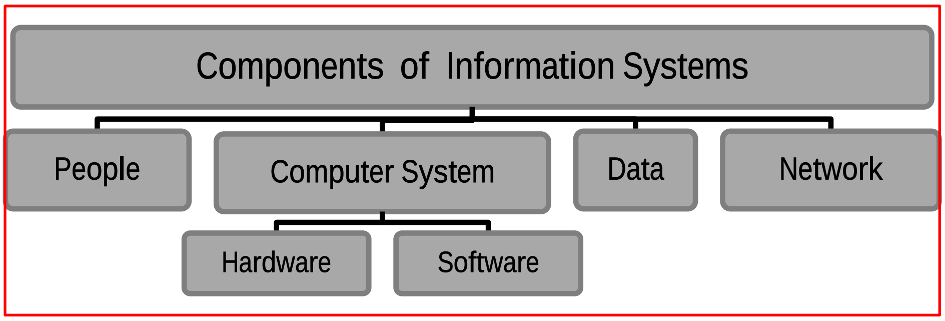


Fig. 2.2 : Components of Information Systems

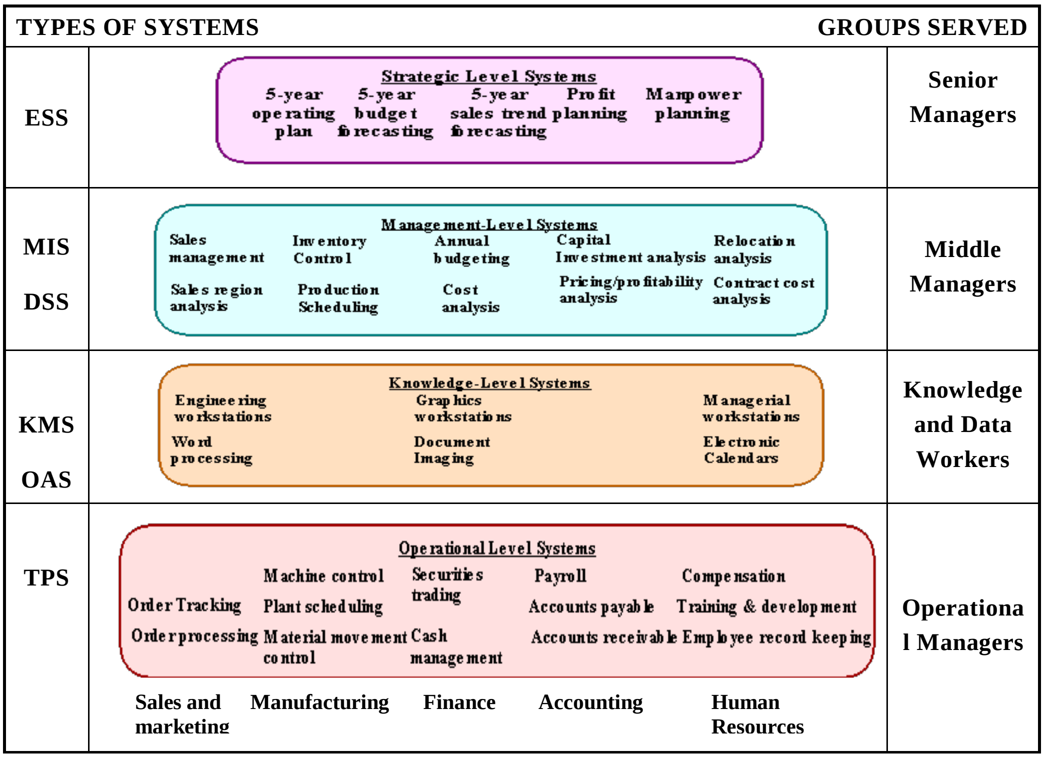
4. Types of Information Systems: Conceptually, information systems are categorized as follows:

4.1 Operations Level Systems: Operations Level Systems produce a variety of information for internal and external use. Their role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database. The main objective of OSS is to improve the operational efficiency of the enterprise. These are further categorized as follows:

(A) Transaction Processing Systems (TPS) - At the lowest level of management, TPS is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for external use. For example, selling a product to a customer will give rise to the need of further information like customer billing, inventory status and increase in account receivable balance. TPS will thus record and manipulate transaction data into usable information.

TPS Components: The principal components of a TPS include inputs, processing, storage and outputs. The components or elements are part of both manual and computerized systems.

Features of TPS: Basic features of TPS are: Large volume of data, Automation of basic operations, Benefits are easily measurable, Source of input for other systems.



TYPES OF SYSTEMS		GROUPS SERVED
ESS	Strategic Level Systems 5-year operating plan 5-year budget forecasting 5-year sales trend forecasting Profit planning Manpower planning	Senior Managers
MIS DSS	Management-Level Systems Sales management Inventory Control Annual budgeting Capital Investment analysis Relocation analysis Sales region analysis Production Scheduling Cost analysis Pricing/profitability analysis Contract cost analysis	Middle Managers
KMS OAS	Knowledge-Level Systems Engineering workstations Graphics workstations Managerial workstations Word processing Document Imaging Electronic Calendars	Knowledge and Data Workers
TPS	Operational Level Systems Machine control Securities trading Payroll Compensation Order Tracking Plant scheduling Accounts payable Training & development Order processing Material movement control Cash management Accounts receivable Employee record keeping Sales and marketing Manufacturing Finance Accounting Human Resources	Operationa l Managers

Fig. 2.3: Types of Information Systems

4.2 Knowledge – Level Systems: These systems support discovery, processing and storage of knowledge and data workers. These support the business to integrate new knowledge into the business and control the flow of paperwork and enable group working.

(A) Office Automation Systems (OAS) – It is most rapidly expanding computer based information systems. Different office activities can be broadly grouped into the following types of operations: Document Capture, Document Creation, Receipts and Distribution, Filling, Search, Retrieval and Follow up, Calculations, Recording Utilization of Resources.

Benefits of OAS can improve communication, reduce the cycle time between preparation of messages and receipt of messages at the recipients' end; reduce the costs of office communication both in terms of time spent by executives and cost of communication links and also ensure accuracy of information and smooth flow of communication. All the activities mentioned have been made very simple, efficient and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

Computer based Office Automation Systems: Major computer based OAS are: Text Processing Systems, Electronic Document Management System, Electronic Message Communication Systems, Teleconferencing and Video-conferencing Systems.

(B) **Knowledge Management Systems –** Knowledge Management (KM) is the process of capturing, developing, sharing, and effectively using organizational knowledge. It refers to a multi-disciplined approach to achieving organizational objectives by making the best use of knowledge. Knowledge Management Systems (KMS) refers to any kind of IT system that stores and retrieves knowledge, improves collaboration, locates knowledge sources, mines repositories for hidden knowledge, captures and uses knowledge, or in some other way enhances the KM process. **Explicit** and **Tacit** are two types of knowledge.

- **Explicit knowledge:** Explicit knowledge is that which can be formalized easily and as a consequence is easily available across the organization.
- **Tacit knowledge:** Tacit knowledge, on the other hand, resides in a few often-in just one person and hasn't been captured by the organization or made available to others.

4.3 **Management Level Systems:** It supports the middle managers in monitoring, decision-making and administrative activities. It provides periodic reports rather than instant information on operations. For example- a college 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 are generally categorized into - **Management Information System (MIS)** and **Decision Support Systems (DSS)**. Each of them is briefly discussed below:

(A) **Management Information Systems (MIS) –** 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 the managers at different levels to take strategic (at top level) or tactical (at middle level) management decisions to fulfill the organizational goals.

Characteristics of an effective MIS: Major characteristic of an effective MIS are:

Management Oriented, Management Directed, Integrated, Common Data Flows, Heavy Planning Element, Sub System Concept, Common Database, Computerized.

Pre-requisites of an Effective MIS – The pre-requisites of an effective MIS are: Database, Qualified System and Management Staff, Support of Top Management, Control and maintenance of MIS.

(B) Decision Support System (DSS) – DSS is a type of computerized information system that supports business and organizational decision-making activities. A Decision Support System (DSS) can be defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own, somewhat personalized, way. A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enable them to generate the information required by them in making decisions. A DSS supports the human decision-making process, rather than a means to replace it.

Planning languages: General-purpose planning languages, Special-purpose planning languages.

Components of DSS – A DSS comprise of four basic components, which are:

- The user: Manager, Staff Specialist (Analysts)
- Databases: Database is implemented at three levels: Physical level, Logical Level, External level.
- Model base: The planning language in a DSS allows the user to maintain a dialogue with the model base, which is the "brain" of DSS because it performs data manipulations and computations with the data provided to it by the user and the database.

Difference between DSS and traditional MIS: Major differences between DSS and traditional MIS are shown in following Table 2. 1.

Table 2.1: Difference between DSS and Traditional MIS

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

4.4 **Strategic Level Systems:** It supports the senior level management to tackle and address strategic issues and long term trends, both inside organization and the outside world.

(A) **Executive Information Systems (EIS) –** It is sometimes referred to as an Executive Support System (ESS). It serves the strategic level i.e. top level managers of the organization. ESS creates a generalized computing and communications environment rather than providing any preset applications or specific competence.

The Executive Decision-Making Environment – The type of decisions that executives must make are very broad. Often, executives make these decisions based on a vision they have regarding 'what it will take to make their enterprise successful.' Some of the characteristics of the types of information used in executive decision making are: Lack of structure, High degree of uncertainty, Future orientation, Informal Source, Low level of detail.

4.5 **Specialized Systems:** Apart from the information systems discussed above, there exists other categories of information systems also that support either operations or management applications. Some of them are Expert Systems, Cross Functional Information Systems, and Core Banking System (CBS) etc. These are briefed as follows:

(A) **Expert Systems -** An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to solve a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such experts. A characteristic of expert systems is the ability to declare or explain the reasoning process that was used to make decisions.

(B) **Cross Functional Information Systems –** It is also known as integrated information system that combines most of information systems and designed to produce information and support decision making for different levels of management and business functions. Example – Enterprise Resource Planning (ERP).

Enterprise Resource Planning (ERP) - Enterprise resource planning (ERP) is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back office functions related to technology, services and human resources. ERP software integrates all facets of an operation, including product planning, development, manufacturing, sales and marketing.

(C) **Core Banking System -** Core Banking System (CBS) may be defined as a back-end system that processes daily banking transactions, and posts updates to accounts and other financial records. These systems typically include deposit, loan and credit-processing capabilities, with interfaces to general ledger systems and reporting tools. Core banking functions differ depending on the specific type of bank. Examples of core banking products include Infosys' Finacle, Nucleus FinnOne and Oracle's Flexcube application (from their acquisition of Indian IT vendor i-flex).

5. Based on the aforementioned facts, the following Table 2.2 describes all the major information systems at-a-glance.

Table 2.2: Different Information Systems

Information System	Description
Transaction Processing Systems (TPS)	These are designed to process and carry out routine transactions efficiently and accurately. A business will have several TPS. For example, Billing systems and invoices to customers, to calculate the weekly and monthly payroll and tax payments of an organization, to calculate raw material requirements, stock control systems to process all movements into, within and out of the business etc.
Office Automation Systems (OAS)	These are systems that help in the enhancement of performance of or productivity of employees who are dealing with the data processing and information. For example, the use of MS-Office can generate the list of customers who have done purchase of certain type of products, number of sales of products done on a particular date etc.
Knowledge Management Systems (KMS)	These help businesses in creation and sharing of information and are typically used in a business where employees create new knowledge and expertise, which can then be shared by other people in the enterprise to create further commercial opportunities. For example, KMS are most effectively used in firms of lawyers, accountants and management consultants. One can say that these are effective in systems, which allow efficient categorization and distribution of knowledge. For example, Knowledge discovery in database and Data mining tools can be used to extract the knowledge from word processing documents, spread sheets, PowerPoint presentations, internet pages, databases, data warehouses.
Decision Support Systems (DSS)	These are specifically designed to help management to make decisions in situations where there is uncertainty about the possible outcomes of those decisions. DSS consists of tools and techniques that gather relevant information and helps in analysis of the options and alternatives. It usually uses complex spread sheet and databases to generate information.

Management Information Systems (MIS)	It is mainly concerned with internal sources of information. It inputs data usually from the transaction processing systems and gives output as a series of management reports. MIS reports can be used by middle management and operational supervisors to gather desired information.
Executive Support System (ESS)	Executive Support System (ESS) is a reporting tool (software) that allows us to turn our organization's data into useful summarized reports. These reports are generally used by executive level managers for quick access to reports coming from all company levels and departments such as billing, cost accounting, staffing, scheduling, and more.

6. Application of Information Systems in Enterprise Processes: Information systems perform following three vital roles in business firms:

- "*Support an organization's business processes and operations":* This includes operations support systems such as Transaction Processing Systems, Process Control Systems.
- *"Support business decision-making":* This includes Management Information Systems, Decision Support Systems, and Executive Information Systems.
- *"Support strategic competitive advantage":* This includes Expert Systems, Knowledge Management Systems, Strategic Information Systems, and Functional Business Systems.

To operate Information Systems (IS) effectively and efficiently, a business manager should have knowledge about Foundation Concepts, Information Technologies (IT), Business Applications, Development Processes, and Management Challenges.

The primary areas where IT enabled tools are used in any organization is shown in Fig. 2.4 whereas Fig. 2.5 showcases different IT enabled tools used at three layers i.e. top, middle and lower management of an organization.

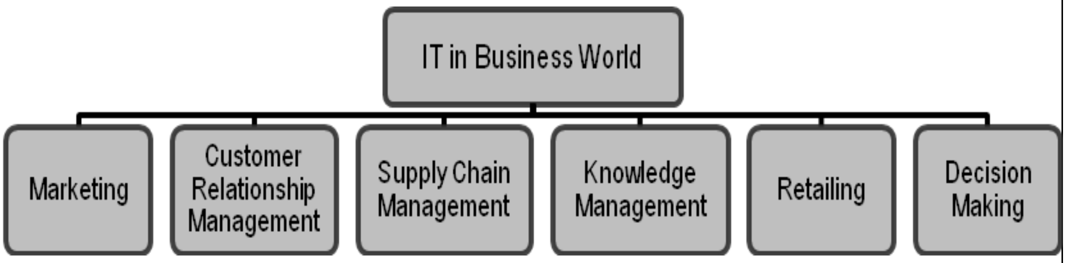


Fig. 2.4: IT in Prime Business Areas

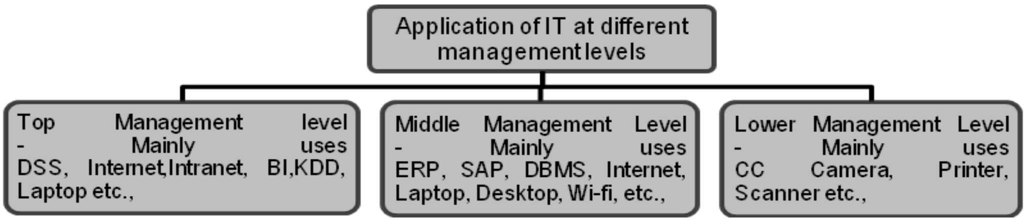

Application of IT at different management levels
Top Management level - Mainly uses DSS, Internet,Intranet, BI,KDD, Laptop etc.,
Middle Management Level - Mainly uses ERP, SAP, DBMS, Internet, Laptop, Desktop, Wi-fi, etc.,
Lower Management Level - Mainly uses CC Camera, Printer, Scanner etc.,

Fig. 2.5: Application of IT at Different Management Levels

7. **Information:** Technically, Information means processed data. Data consists of facts, values or results, and information is the result of relations between data e.g. in a spread sheet, student name, roll number and marks obtained in science and arts subjects represent 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.

Information is data that have been put into a meaningful and useful context. Mere collection of data is not information and mere collection of information is not knowledge.

7.1 **Attributes of Information:** These are - Availability, Purpose, Mode and Format, Decay-Rate, Frequency, Completeness, Reliability, Cost-benefit Analysis, Validity, Quality, Transparency, and Value of Information.

8. **Role of Information in Business:** The information can be categorized on the basis of its requirement by the top, middle and lower level management as seen in Fig. 2.6. The top management generally comprise of owners/shareholders, board of directors, its chairman, managing director, or the chief executive, or the managers committee having key officers, the middle management comprise of heads of functions departments e.g. purchase manager, production manager, marketing managers, financial controller, and divisional sectional officers working under these functional heads, whereas the lower level managers are superintendents, supervisor, etc.

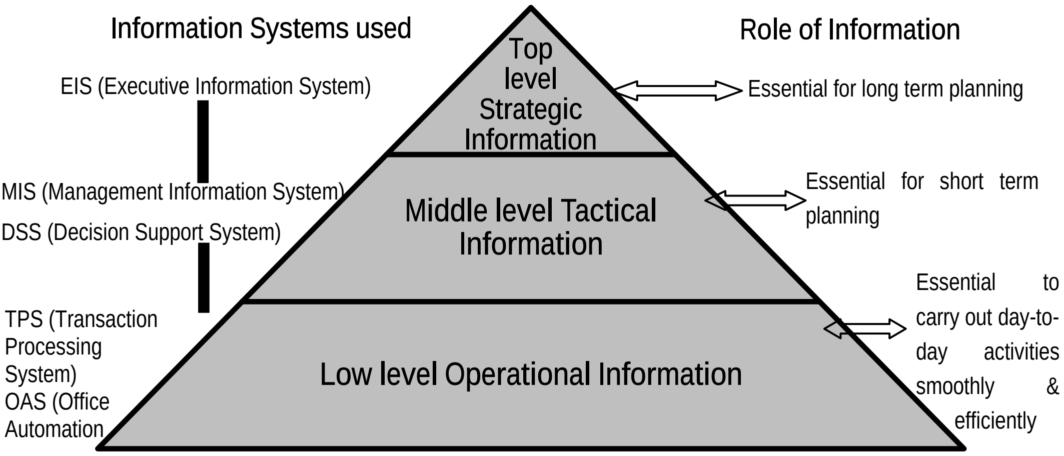

Information Systems used
Role of Information
Top level Strategic Information
Middle level Tactical Information
Low level Operational Information
EIS (Executive Information System)
MIS (Management Information System)
DSS (Decision Support System)
TPS (Transaction Processing System)
OAS (Office Automation
Essential for long term planning
Essential for short term planning
Essential to carry out day-to-day activities smoothly & efficiently

Fig. 2.6: Types of Information Systems at Different Management Levels

9. Relative Importance of Information Systems from Strategic and Operational Perspectives:

In this age of technology and competition, enterprises are looking for novel ideas and information that can enhance and expand their business. In order to achieve this, they are becoming more and more dependent on information systems. Information system is used in every aspects of business right from customer relationship management, marketing strategies, retailing, communication, product promotion, product development, forecast future sales to supply chain management etc. ERP, Data Mining tools, Data warehouse, Business intelligence, MIS, internet, intranet, extranet etc. are the information systems and information technologies that support managers in every step of business.

Information Systems have accelerated the pace of processing of enterprise information using IT and integrating all aspects of the operations of the business e.g. instead of gathering data manually and taking out hidden information from it by conducting meeting of executives, which is crucial in decision making for marketing strategies, customer relationship management etc., the same can be obtained by using the respective data mining tools and data warehouse. Not only this, Information System also provides new platform to business world where space and time is no more obstacle. For example, selling and purchasing of products can be done on web any time and from anywhere.

10. Overview of Underlying IT Technologies: Major IT tools crucial for business growth are: Business Website, Internet and Intranet, Software Packages, Computer Systems, Scanners, Laptop, Printer, Webcam, Smart Phone etc.

Question 1

Define the following terms briefly:

(a) Abstract System

(b) Physical System

(c) Open System

(d) Closed System

(e) Deterministic System

(f) Probabilistic System

Answer

(a) Abstract System: Abstract System also known as Conceptual System or Model can be defined as an orderly arrangement of interdependent ideas or constructs. For example, a system of theology is an orderly arrangement of ideas about God and the relationship of humans to God.

(b) Physical System: Physical System is a set of tangible elements, which operate together to accomplish an objective e.g. Computer system, University system etc.

(c) Open System: An Open System interacts with other systems in its environment and changes with changes in the environment. For example; Information system is an open system because it takes input from the environment and produces output to the environment, which changes as per the changes in the environment.

(d) Closed System: A Closed System does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of a number of components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation.

(e) Deterministic System: A Deterministic System operates in a predictable manner. For example; software that performs on a set of instructions is a deterministic system.

(f) Probabilistic System: A Probabilistic System can be defined in terms of probable behaviour. For example; inventory system is a probabilistic system where the average demand, average time for replenishment, etc. may be defined, but the exact value at any given time is not known.

Question 2

Discuss important characteristics of Computer based Information Systems in brief.

Answer

Major characteristics of Computer based Information Systems are given as follows:

- All systems work for predetermined objectives and the system is designed and developed accordingly.
- In general, a system has a number of interrelated and interdependent subsystems or components. No subsystem can function in isolation; it depends on other subsystems for its inputs.
- If one subsystem or component of a system fails; in most of the cases, the whole system does not work. However, it depends on 'how the subsystems are interrelated'.
- The way a subsystem works with another subsystem is called interaction. The different subsystems interact with each other to achieve the goal of the system.
- The work done by individual subsystems 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.

Question 3

What do you understand by TPS? Briefly discuss the key activities involved in a TPS.

Answer

Transaction Processing System (TPS): At the lowest level of management, TPS is an information system that manipulates data from business transactions. Any business activity such as sales, purchase, production, delivery, payments or receipts involves transaction and these transactions are to be organized and manipulated to generate various information products for internal and external use. For example, selling of a product to a customer will give rise to the need of further information like customer billing, inventory status and increase in account receivable balance. TPS will thus record and manipulate transaction data into usable information.

Major activities involved in a TPS are given as follows:

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

Question 4

What are the principal components of a TPS? Discuss in brief.

Answer

TPS Components: The principal components of a TPS are given as follows:

- **Inputs –** Source documents, such as customer orders, sales, slips, invoices, purchase orders, and employee time cards, are the physical evidence of inputs in to the Transaction Processing System. They serve several purposes like capturing data, facilitating operations by communicating data and authorizing another operation in the process, standardizing operations by indicating, which data require recording and what actions need to be taken and providing a permanent file for future analysis, if the documents are retained etc. Input of transactions may also be done in electronic form e.g. swiping and attendance card.
- **Processing –** This involves the use of journals and registers to provide a permanent and chronological record of inputs. Journals are used to record financial accounting transactions, and registers are used to record other types of data not directly related to accounting. Some of the common journals are sales journal, purchase journal, cash receipts journal etc.
- **Storage –** Ledgers and files provide storage of data on both manual and computerized systems. The general ledger, the accounts payable ledger, and the accounts receivable ledger are some of the records of a firm's financial accounting transactions.
- **Outputs –** Any document generated from the system is output. Some documents are both output and input. For example; a customer invoice is an output from the order-entry

application system and also and input document to the customer. Financial reports summarize the results of transaction processing and express these results in accordance with the principles of financial reporting.

Question 5

Explain basic features of a TPS in brief.

Answer

Basic features of TPS are given as follows:

- **Large volume of data-** As TPS is transaction oriented and generally consists of large volumes of data, it requires greater storage capacity. Their primary objective is to ensure that the data regarding the economic events in the enterprises are captured quickly and correctly.
- **Automation of basic operations-** Any TPS aims at automating the basic operations of a business enterprise and plays a critical role in its day-to-day functioning. 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 of the enterprise.
- **Benefits are easily measurable-** TPS reduces the workload of the people associated with 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, 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.

Question 6

What do you understand by MIS? Discuss major characteristics of an effective MIS.

Answer

Management Information Systems (MIS): 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 an effective MIS: Major characteristics of an effective MIS are given as follows:

- Management Oriented: It means that efforts for the development of the Information System should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management.
- Management Directed: Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote sufficient amount of their time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- Integrated: The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are to be tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
- Common Data Flows: It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
- Heavy Planning Element: An MIS usually takes one to three years and sometimes even longer to get established firmly within a company. Therefore, a MIS designer must be present while development of MIS and should consider future enterprise objectives and requirements of information as per its organization structure.
- Sub System Concept: Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time in a phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- Common Database: Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of

duplication in data storage, updating, deletion and protection.

- **Computerized:** Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in MIS.

Question 7

Briefly discuss major misconceptions about MIS.

Answer

Following are the major misconceptions about MIS:

- Any computer based information system is a MIS.
- Any reporting system is MIS.
- MIS is a management technique.
- MIS is a bunch of technologies.
- MIS is an implementation of organizational systems and procedures. It is a file structure.
- The study of MIS is about use of computers.
- More data in reports generated results in more information to managers.
- Accuracy plays vital role in reporting.

Question 8

'There are various constraints, which come in the way of operating an MIS'. Explain any four such constraints in brief.

Answer

Four major constraints, which come in the way of operating an MIS, are given as follows:

- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing a system, which operates properly. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
- Experts usually face the problem of selecting which sub-system of MIS should be installed and operated first. The criteria, which should guide the experts, depend its need and importance.
- Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is no-standardized.

- Non-cooperation from staff is a crucial problem, which should be handled tactfully. This can be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some staff should also be involved in the development and implementation of the system to buy-in their participation.

Question 9

What are major limitations of MIS? Explain in brief.

Answer

Major Limitations of MIS are given as follows:

- The quality of the outputs of MIS is basically governed by the quality of input and processes.
- MIS is not a substitute for effective management, which means that it cannot replace managerial judgment in making decisions in different functional areas. It is merely an important tool in the hands of executives for decision making and problem solving.
- MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in fast changing and complex environment.
- MIS cannot provide tailor-made information packages suitable for every type of decision made by executives.
- MIS takes into account mainly quantitative factors, thus it ignores the non-quantitative factors like morale and attitude of members of organization, which have an important bearing on the decision making process of executives or senior management.
- MIS is less useful for making non-programmed decisions. Such decisions are not routine and thus require information, which may not be available from existing MIS.
- The effectiveness of MIS is reduced in enterprises, where the culture of hoarding information and not sharing with other is prevalent.
- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

Question 10

What is Decision Support System (DSS)? Explain the key characteristics of a DSS in brief.

Answer

Decision Support System (DSS): A DSS can be defined as a system that provides tools to managers to assist them in solving semi-structured and unstructured problems in their own, somewhat personalized, way. A DSS is not intended to make decisions for managers, but rather to provide managers with a set of capabilities that enable them to generate the information required by them to make decisions. A DSS supports the human decision-making process, rather than becoming a means to replace it.

Characteristics of DSS: The key characteristics of a DSS are given as follows:

- This supports decision making and occurs at all levels of management.
- Instead of helping individuals working on independent tasks, it should be able to help groups in decision making.
- It should be flexible and adaptable. i.e. it should be able to fit itself in the style of a particular manager and ready to change according to changes in the environment.
- DSS focuses on decisions rather than data and information.
- It should be easy to use. A user should not need to have knowledge of computer programming to generate reports that help in decision making.
- DSS can be used for solving structured problems.
- DSS should be user-friendly.
- DSS should be extensible and evolve over-time.
- DSS is used mainly for decision making rather than communicating decisions and training purposes.
- The impact of DSS should be on decision where the manager's judgment is essential and there is sufficient structure suitable for using computer systems.

Question 11

Discuss various examples of DSS in Accounting.

Answer

Examples of Decision Support Systems (DSS) in Accounting: DSSs are widely used as a part of an organization's Accounting Information System. The complexity and nature of decision support systems 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. Decision support systems can accumulate these product costs to calculate total costs per patient. Health care managers many combine cost accounting decision support systems 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 decision support system 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 decision support system 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 decision support system, accountants, managers, and engineers identify and prioritize these factors. They can then evaluate up to seven investment alternatives at once.
- **Budget Variance Analysis System:** Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized decision support system 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 decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.
- **General Decision Support System:** As mentioned earlier, some planning languages used in decision support systems are general purpose and therefore have the ability to analyze many different types of problems. In a sense, these types of decision support systems 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 decision support system. 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 decision support system 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.

Question 12

What is Executive Information System (EIS)? Explain its major characteristics.

Answer

Executive Information Systems (EIS): It is sometimes referred to as an Executive Support System (ESS) too. It serves the strategic level i.e. top level managers of the organization. ESS creates a generalized computing and communications environment rather than providing any preset applications or specific competence.

Characteristics of EIS: Major Characteristics of an EIS are given as follows:

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

Question 13

'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.

Answer

The principles to guide the design of measures and indicators to be included in an EIS are given as follows:

- 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 reflect 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.

Question 14

Discuss the difference between Executive Information System (EIS) and Traditional Information Systems.

Answer

Major differences between Executive Information System (EIS) and Traditional Information Systems are shown in the following Table:

Table: Difference between EIS and Traditional Information Systems

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

Question 15

What is an Expert System? Discuss some of the business implications of Expert Systems in brief.

Answer

Expert System: An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to solve a problem. Expert System is software system that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such experts. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities? And so on. Based on the answers given by client, it may suggest a suitable portfolio.

A characteristic of Expert System is its ability to declare or explain the reasoning process that was used to make decisions. Some of the business applications of Expert System are given a follows:

- **Accounting and Finance:** It provides tax advice and assistance, helping with credit-authorization decisions, selecting forecasting models, providing investment advice.
- **Marketing:** It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.
- **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 facility layouts.
- **Personnel:** It is useful in assessing applicant qualifications, giving employees assistance in filling out forms.
- **General Business:** It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, evaluating performance.

Question 16

Describe the major benefits of Expert Systems in brief.

Answer

Major benefits of expert systems are given as follows:

- Expert Systems preserve knowledge that might be lost through retirement, resignation or death of an acknowledged company expert.
- Expert Systems put information into an active-form so that it can be summoned almost as a real-life expert might be summoned.
- Expert Systems assist novices in thinking the way experienced professionals do.
- Expert Systems are not subjected to such human fallings as fatigue, being too busy, or being emotional.
- Expert Systems can be effectively used as a strategic tool in the areas of marketing products, cutting costs and improving products.

Question 17

Discuss some of the important implications of Information Systems in business.

Answer

Following are some of the important implications of Information Systems in business:

- Information Systems help managers in efficient decision-making to achieve organizational goals.

- An organization will be able to survive and thrive in a highly competitive environment on the strength of a well-designed Information system.
- Information Systems help in making right decision at the right time i.e. just on time.
- A good Information System may help in generating innovative ideas for solving critical problems.
- Knowledge gathered though Information systems may be utilized by managers in unusual situations.
- Information System is viewed as a process; it can be integrated to formulate a strategy of action or operation.

Question 18

What is Information? Briefly discuss its attributes.

Answer

Information: 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:

- **Availability –** It is a very important aspect of information. Information is useless if it is not available at the time of need.
- **Purpose/Objective –** Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. Depending upon the activities in an organization the Information communicated to people has a purpose. 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.

- Mode and format – The modes of communicating information to humans should be in such a way that it can be easily understand by the people. The mode may be in the form of voice, text or a combination of these two. Format also plays an important role in communicating the idea. It should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information, different formats can be used e.g. diagrams, graphs, curves are best suited for representing statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.
- Current/Updated – 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.
- Rate – The rate of transmission/reception of information may be represented by the time required to understand a particular situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. For example- information available from internet site should be available at a click of mouse, and one should not have to wait for it for an hour.
- Frequency – The frequency with which information is transmitted or received affects its value. For example- weekly reports of sales show little change as compared to the quarterly reports and contribute less for assessing salesman capability.
- Completeness and Adequacy – The information provided should be complete and adequate in itself because only complete information can be used in policy making. For example-the position of student in a class can be found out only after having the information of the marks of all students and the total number of students in a class.
- 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.
- 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.
- Quality – It means the correctness of information. For example, the correct status of inventory is highly required.
- 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.

- 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.

Question 19

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.

Answer

Expert System: An Expert System is highly developed Decision Support System (DSS) that utilizes the knowledge generally possessed by an expert to solve a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like – how much can be invested. Does the client have any preferences regarding specific types of securities?

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.*

Question 20

Write a short note on the Operating System Security.

Note: Students are advised to read this question while referring to chapter number 3 as the question pertains to that chapter.

Answer

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 defence 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 Operating System 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.*

Question 21

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

Answer

Office Automation Systems (OAS) is most rapidly expanding computer based information systems. The broad groups that can be formed on the basis of its operations are as follows:

(i) Text processing system: The text processing system automates the process of document capture and/ or creation of new documents such as letters, reports, memo etc. This permits use of standard stored information to produce personalized documents. It reduces effort and minimizes the chances of errors.

(ii) Electronic Document Management system: It captures the information contained in documents, stored for future reference and makes them available to the users as and when required. These systems are very helpful in remote access of documents

and internal communication through network. It also helps to keep record of resources utilization.

(iii) Electronic message communication system: The electronic message communication system helps in receipts and distribution of electronic records. It offers a lot of economy in terms of reduced time in sending or receiving the message; online development and editing; broadcasting and rerouting; and integration with other information system. E-mail, Fax, and voice mail are important OAS.

(iv) Teleconferencing and Video Conferencing systems: 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.

Question 22

A business manager should have adequate knowledge to operate Information Systems effectively. Elaborate.

Answer

To operate Information Systems (IS) effectively and efficiently, a business manager should have following knowledge about it.

- *Foundation Concepts – 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) – 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.*

Question 23

Modern business used 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.

Answer

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.*

Exercise

1. *What is DSS? Explain the components of a DSS in brief.*
2. *Differentiate between DSS and Traditional MIS.*
3. *“A Decision Support System supports human decision-making process rather than providing a means to replace it”. Justify the above statement by stating the characteristics of decision support system.*

4. *"Decision support systems are widely used as part of an Organization's Accounting Information system". Give examples to support this statement.*

5. *Briefly describe five major characteristics of the types of information used in Executive Decision making.*

6. *Write short notes on the following:*

   (i) Text Processing Systems

   (ii) Components of Message Communication Systems

   (iii) Teleconferencing and Video-conferencing Systems

   (iv) Role of information in business

7. *Describe the main pre-requisites of a Management Information System, which makes it an effective management tool.*

8. *Distinguish between General-purpose planning languages and Special-purpose Planning Languages.*

3

Protection of Information Systems

Basic Concepts

1. Need for Protection of Information Systems: Information security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information. That is why protection of information systems has become a need for organizations.

2. Information System Security: Information security refers to the protection of valuable assets against loss, disclosure, or damage. For any organization, the security objective comprises three universally accepted attributes:

- **Confidentiality:** Prevention of the unauthorized disclosure of information;
- **Integrity:** Prevention of the unauthorized modification of information; and
- **Availability:** Prevention of the unauthorized withholding of information.

The relative priority and significance of Confidentiality, Integrity and Availability (CIA) vary according to the data within the information system and the business context in which it is used.

2.1 What Information is Sensitive?

The common aspect in each organization is the critical information that each organization generates. These are: Strategic Plans, Business Operational data and Financial records etc.

3. Information Security Policy: An Information Security policy is the statement of intent by the management about how to protect a company's information assets. It is a formal statement of the rules, which govern access to people to an organization's technology and information assets, and which they must abide by.

Major Information Security Policies are: Information Security Policy, User Security Policy, Acceptable Usage Policy, Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy.

4. Information Systems Controls: 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. Thus, information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

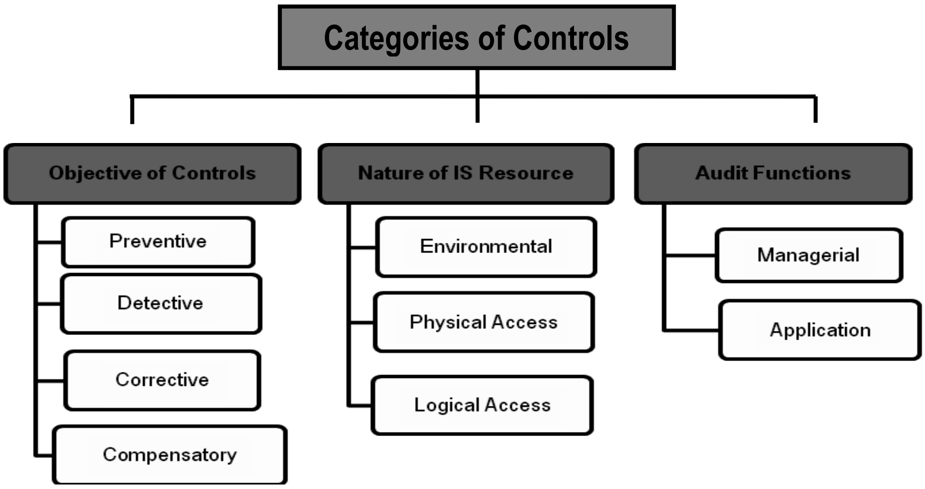
4.1 Impact of Technology on Internal Controls: The internal controls within an enterprise in a computerized environment encompass the goal of asset safeguarding, data integrity, system efficiency and effectiveness. These are: Personnel, Segregation of duties, Authorization procedures, Record keeping, Access to assets and records, Management supervision and review, Risks due to concentration of programs and data.

Internal controls comprise of the following five interrelated components: Control Environment, Risk Assessment, Control Activities, Information and Communication, Monitoring.

4.2 Objective of Controls: The objective of controls is to reduce or if possible eliminate the causes of exposure to potential loss.

5. Categories of Controls

Controls can be classified into following categories as shown in the Fig. below:



(a) Based on the objective of controls, these can be classified as under:

(i) **Preventive Controls:** Preventive controls are those, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system.

(ii) **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend.

(iii) **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control.

(iv) **Compensatory Controls:** Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. 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*."

(b) Another classification of controls is based on the nature of IS resource. These are given as follows:

(i) **Environmental Controls:** These are the controls relating to IT environment such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc. These are related to the external factors in the Information Systems and preventive measures to overcome the conflicts. The controls over environment exposures are: Water Detectors, Hand-Held Fire Extinguishers, Manual Fire Alarms, Smoke Detectors, Fire Suppression Systems, Strategically Locating the Computer Room, Regular Inspection by Fire Department, Fireproof Walls, Floors and Ceilings surrounding the Computer Room, Electrical Surge Protectors, Uninterruptible Power System (UPS)/Generator, Power Leads from Two Substations, Emergency Power-Off Switch, Wiring Placed in Electrical Panels and Conduit, Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility, Fire Resistant Office Materials and Documented and Tested Emergency Evacuation.

(ii) **Physical Access Controls:** These are the controls relating to physical security of tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc. These controls are personnel; hardware and include procedures exercised on access to IT resources by employees/outsiders. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy. These controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons. These are as follows:

(a) **Locks on Doors -** Cipher locks (Combination Door Locks) , Bolting Door and Electronic Door Locks.

(b) **Physical Identification Medium -** Personal Identification numbers (PIN), Plastic Cards Identification Badges.

(c) **Logging on Facilities -** Manual Logging and Electronic Logging.

(d) **Other means of Controlling Physical Access -** Video Cameras, Security Guards, Controlled Visitor Access, Bonded Personnel, Dead Man Doors, Non–exposure of Sensitive Facilities, Computer Terminal Locks, Controlled Single Entry Point, Alarm System, Perimeter Fencing, Control of out of hours of employee-employees and Secured Report/Document Distribution Cart.

(iii) **Logical Access Controls:** These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc. are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss.

- **Logical Access Paths:** These are Online Terminals, Dial-up Ports and Telecommunication Network etc.
- **Issues and Revelations related to Logical Access:** Compromise or absence of logical access controls in the organizations may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposures of logical access control encourage technical exposures and computer crimes. These are as follows:
  - **Technical Exposures:** Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include: Data Diddling, Bombs- Time Bomb & Logic Bomb, Trojan Horse, Worms, Rounding, Salami Techniques and Trap Doors.
  - **Computer Crime Exposures:** Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations. These are: Financial Loss, Legal Repercussions, Loss of Credibility or Competitive Edge, Blackmail/Industrial Espionage, Disclosure of Confidential, Sensitive or Embarrassing Information, Sabotage and Spoofing.
  - **Asynchronous Attacks:** They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data can be transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. There are many forms of asynchronous attacks, some of them are: Data Leakage, Wire-tapping, Piggybacking and Shutting Down of the Computer/Denial of Service.
- **Logical Access Control across the System:** The purpose of logical access controls is to restrict access to information assets/resources. They are expected to provide access to information resources on a need to know and need to do

basis using principle of least privileges. These are: User access management, User responsibilities, Network access control, Operating system access control, Application and monitoring system access control and Mobile computing related controls.

(c) Classification on the basis of "Audit Functions" – Managerial Controls and Application Controls

(i) Managerial Controls: These are the controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.

- **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.
- **Information Systems 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.
- **Systems Development Management:** Systems Development Management is responsible for the design, implementation, and maintenance of application systems.
- **Programming Management:** It is responsible for programming new system; maintain old systems and provides general systems support software.
- **Data Administration:** Data administration is responsible for addressing planning and control issues in relation to use of an organization's data.
- **Quality Assurance Management:** It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.
- **Security Administration:** It is responsible for access controls and physical security over the information systems function.
- **Operations Management:** It is responsible for planning and control of the day-to-day operations of information systems.

(ii) Application Controls: Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. Application Control Techniques include the programmatic routines within the application program code. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage.

These are – Boundary Controls, Input Controls, Communication Controls, Processing Controls, Database Controls and Output Controls.

- **Boundary Controls:** Major controls of the boundary system are the access control mechanisms. Access control mechanism links authentic users to authorized resources that they are permitted to access. Major Boundary Control techniques are Cryptography, Passwords, Personal Identification Numbers (PIN), Identification Cards and Biometric Devices.
- **Input Controls:** These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system.
- **Communication Controls:** 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.
- **Processing Controls:** Data processing controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed.
- **Database Controls:** Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called update controls and report controls. Major update controls are: Sequence Check between Transaction and Master Files, Ensure All Records on Files are processed, Process multiple transactions for a single record in the correct order and maintain a suspense account.
- **Output Controls:** These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner. Output can be in any form, it can either be a printed data report or a database file in a removable media such as a CD-ROM or it can be a Word document on the computer's hard disk.

  Major Report controls are: Standing Data, Print-Run-to Run control Totals, Print Suspense Account Entries and Existence/Recovery Controls.

6. General Controls: Information Technology General Controls (ITGC) are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions.

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

8. Controls over Data Integrity and Security: The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through various stages of a specific data processing program. There are six categories of integrity controls: Source data control, Input validation routines, On-line data entry controls, Data processing and storage controls, Output controls and Data Transmission controls.

Data Integrity Policies: Major data integrity policies are: Virus-Signature Updating, Software Testing, Division of Environments etc.

9 Cyber Frauds: Cyber Fraud shall mean fraud committed by use of technology. Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online. The most common form is online credit card theft. On the basis of the functionality, these are of two types:

- **Pure Cyber Frauds:** Frauds, which exist only in cyber world. They are borne out of use of technology. For example: Website hacking.
- **Cyber Enabled Frauds:** Frauds, which can be committed in physical world also but with use of technology; the size, scale and location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.

9.1 Cyber Attacks: Major cyber-attacks are: Phishing, Network Scanning, Virus/Malicious Code, Spam, Website Compromise/Malware Propagation and others like Cracking, Eavesdropping, E-mail Forgery, E-mail Threats and Scavenging.

9.2 Impact of Cyber Frauds on Enterprises: The impact of cyber frauds on enterprises can be viewed under the following dimensions: Financial Loss, Legal Repercussions, Loss of credibility or Competitive Edge, Disclosure of Confidential, Sensitive or Embarrassing Information and Sabotage.

9.3 Techniques to Commit Cyber Frauds: These are: Hacking, Cracking, Data Diddling, Data Leakage, Denial of Service (DoS) Attack, Internet Terrorism, Logic Time Bombs, Masquerading or Impersonation, Password Cracking, Piggybacking, Round Down, Scavenging or Dumpster Diving, Social Engineering Techniques, Super Zapping and Trap Door.

In spite of having various controls as well as countermeasures in place, cyber frauds are happening and increasing on a continuous basis. To overcome these frauds, there is an urgent need to conduct research in the related areas and come up with more appropriate security mechanisms, which can make information systems more secure.

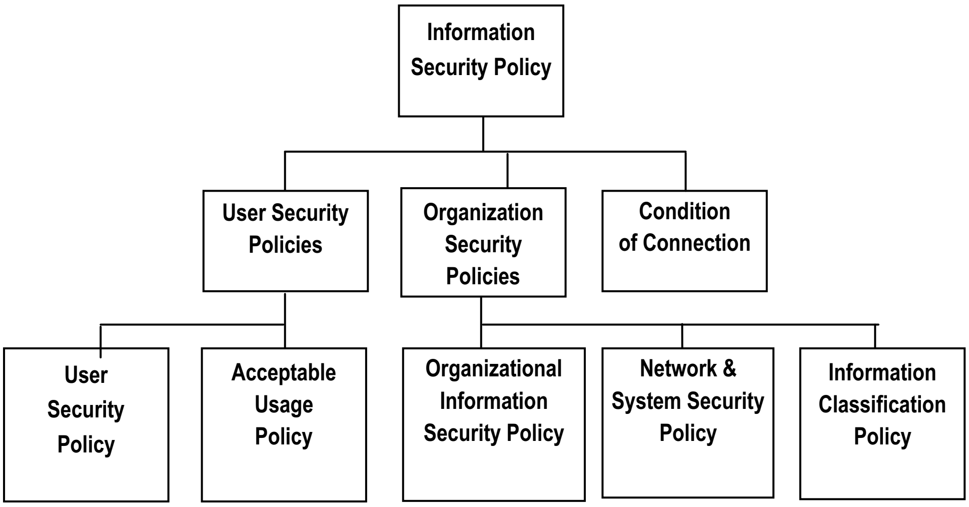
Question 1

Discuss various types of Information Security polices and their hierarchy.

Answer

Various types of information security policies are as follows:

- **Information Security Policy –** This policy provides a definition of Information Security, its overall objective and the importance that applies to all users.
- **User Security Policy –** This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
- **Acceptable Usage Policy –** This sets out the policy for acceptable use of email, Internet services and other IT resources.
- **Organizational Information Security Policy –** This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
- **Network & System Security Policy –** This policy sets out detailed policy for system and network security and applies to IT department users.
- **Information Classification Policy –** This policy sets out the policy for the classification of information.
- **Conditions of Connection –** This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.


Information Security Policy
User Security Policies
Organization Security Policies
Condition of Connection
User Security Policy
Acceptable Usage Policy
Organizational Information Security Policy
Network & System Security Policy
Information Classification Policy

The hierarchy of Information Security Policies

Question 2

What are the key components of a good security policy? Explain in brief.

Answer

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 Compliance; and
- Monitoring and Auditing Requirements.

Question 3

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."

Discuss Information Security Policy and also identify the salient components that have not been covered in the above policy.

Answer

A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets including sensitive information are managed, protected, and distributed within the user organization.

An Information Security Policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls, who owns the information, and authority issues.

Issues to address: This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by an appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities, and
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

In the stated scenario of the question, the ISMS Policy of the given organization does not address the following issues:

- Definition of information security,
- Reasons why information security is important to the organization,
- A brief explanation of the security policies, principles, standards and compliance, and
- Reference to supporting documents.

Question 4

What do you mean by Preventive Controls? Explain with the help of examples. Also discuss their broad characteristics in brief.

Answer

Preventive Controls: Preventive controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to a financial system. These can be implemented in both manual and computerized environment for the same purpose. Only, the implementation methodology may differ from one environment to the other. Examples of preventive controls are given as follows:

- Employ qualified personnel,
- Segregation of duties,
- Access control,
- Vaccination against diseases,
- Documentation,
- Prescribing appropriate books for a course,
- Training and retraining of staff,
- Authorization of transaction,
- Validation, edit checks in the application,
- Firewalls,
- Anti-virus software (sometimes this acts like a corrective control also), etc., and
- Passwords.

The above list contains both manual and computerized, preventive controls.

The broad characteristics of preventive controls are given as follows:

- A clear-cut understanding about the vulnerabilities of the asset;
- Understanding probable threats; and
- Provision of necessary controls to prevent probable threats from materializing.

Question 5

What do you mean by Corrective Controls? Explain with the help of examples. Also discuss their broad characteristics in brief.

Answer

Corrective Controls: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control.

Examples of Corrective Controls are given as follows:

- Contingency planning,
- Rerun procedures,
- Change input value to an application system, and
- Investigate budget variance and report violations.

The main characteristics of the corrective controls are given as follows:

- 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 processing systems to minimize future occurrences of incidents.

Question 6

What do you understand by Financial Controls? Explain major financial control techniques in brief.

Answer

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

Major financial control techniques are given as follows:

- **Authorization:** This entails obtaining the authority to perform some act typically accessing such assets as accounting or application entries.
- **Budgets:** These are estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
- **Cancellation of documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a “paid” or “processed” stamp or punching a hole in the document.
- **Documentation:** This includes written or typed explanations of actions taken on specific transactions; it also refers to written or typed instructions, which explain the performance of tasks.

- **Dual control:** This entails having two people simultaneously access an asset. For example, the depositories of banks' 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.
- **Input/ output verification:** This entails comparing the information provided by a computer system with the input documents. This is an expensive control that tends to be over-recommended by auditors.
- **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
- **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enables the detection of missing documents.
- **Supervisory review:** This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them. This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

Question 7

What do you understand by Boundary Controls? Explain major Boundary Control techniques in brief.

Answer

Boundary Controls: The major controls of the boundary system are the access control mechanisms. Access control mechanism links authentic users to resources, they are permitted to access. The access control mechanism has three steps of identification, authentication and authorization with respect to the access control policy.

Major Boundary Control techniques are given as follows:

- **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst. Three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution).
- **Passwords:** User identification by an authentication mechanism normally with strong password may be a good boundary access control. A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common

dictionary words, periodic change of passwords, hashing of passwords and number of unsuccessful entry attempts.

- **Personal Identification Numbers (PIN):** PIN is similar to a password. It is assigned to a user by an institution using a random number stored in its database and sent independently to a user after identification. It can also be a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
- **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
- **Biometric Devices:** Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

Question 8

Briefly explain major update and report controls with reference to Database Controls in brief.

Answer

Major update controls are given as follows:

- **Sequence Check between Transaction and Master Files:** Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updation, insertion or deletion of records in the master file with respect to the transaction records. If errors in this stage are overlooked, it leads to corruption of critical data. For example, transaction on a new inventory item should be processed only after the creating the inventory master record for the item.
- **Ensure All Records on Files are processed:** During processing, ensure that all the transactions till the end of the file marker are processed and similarly when processing master records, all records till end to master file marker are processed.
- **Process multiple transactions for a single record in the correct order:** 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 e.g. chronological order.
- **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. If the suspense account has a non-zero balance, it reflects the errors to be corrected.

Major Report controls are given as follows:

- **Standing Data:** Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. 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 control Totals:** Run-to-Run control totals help 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 monitored with the respective error file and action taken on time.
- **Existence/Recovery Controls:** The back-up and recovery strategies together encompass the controls required to restore failure in a database. Backup strategies are implemented using prior version and logs of transactions or changes to the database. Recovery strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

Question 9

What do you understand by classification of Information? Explain different classifications of Information.

Answer

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:

- **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.
- **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.

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

Question 10

Briefly explain major Data Integrity Policies.

Answer

Major Data Integrity Policies are given as under:

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

Question 11

Write short notes on the following:

(i) Time Bomb

(ii) Logic Bomb

(iii) Trojan Horse

(iv) Worms

Answer

(i) Time Bomb: This name has been borrowed from its physical counterpart because of mechanism of activation. A physical time bomb explodes at the time it is set for (unless somebody forces it to explode early), likewise the computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.

(ii) Logic Bomb: They resemble time bombs in their destruction activity. Logic bombs are activated by combination of events. For example, a code like; "If a file named DELETENOT is deleted then destroy the memory contents by writing ones." This code segment, on execution, may cause destruction of the contents of the memory on deleting a file named DELETENOT. These bombs can be set to go off at a future event.

(iii) Trojan Horse: These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it. A Trojan may:

- Change or steal the password or
- May modify records in protected files or
- May allow illicit users to use the systems.

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

Christmas Card is a well-known example of Trojan. It was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network. Because of this message on other terminals, other users cannot save their half finished work.

(iv) Worms: A worm does not require a host program like a Trojan to replicate itself. Thus, a Worm program copies itself to another machine on the network. Since worms are stand-alone programs, they can be detected easily in comparison to Trojans and computer viruses.

Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock worm places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive. Existential worm does not cause damage to the system, but only copies itself to several places in a computer network.

Question 12

What do you understand by Asynchronous Attacks? Explain various forms of Asynchronous Attacks in brief.

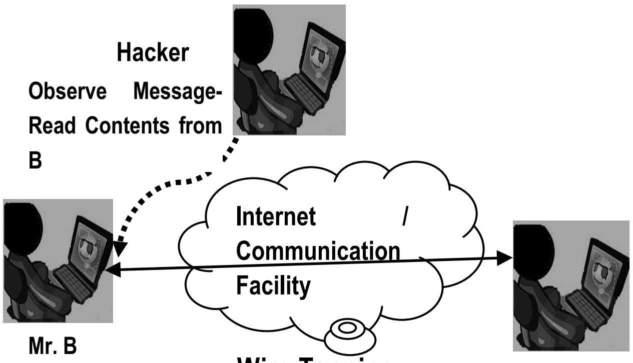
Answer

Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions.

There are many forms of asynchronous attacks; some of them are given as follows:

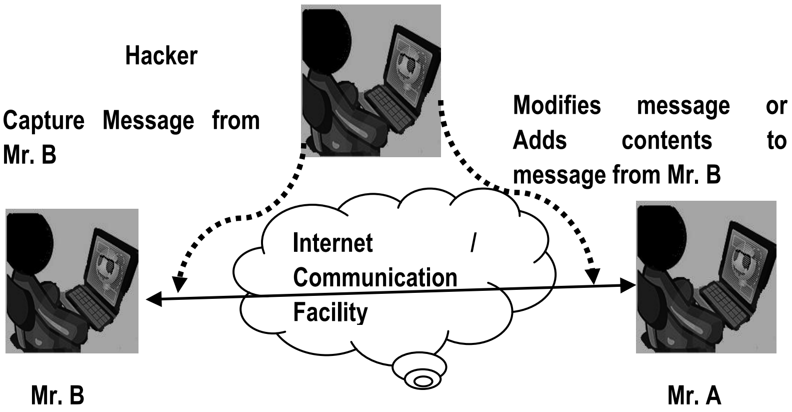
(i) **Data Leakage:** Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.

(ii) **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.


Hacker
Observe Message-Read Contents from B
Internet / Communication Facility
Mr. B
Mr. A

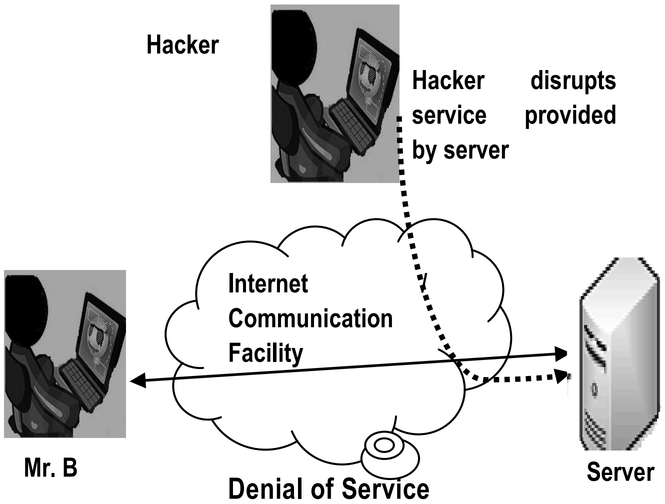
Wire Tapping

(iii) **Piggybacking:** This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages.


Hacker
Capture Message from Mr. B
Modifies message or Adds contents to message from Mr. B
Internet / Communication Facility
Mr. B
Mr. A

Piggybacking

(iv) **Shutting Down of the Computer/Denial of Service:** This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals, who know the high-level systems log on-ID initiate shutting down process. The security measure will function effectively if there are appropriate access controls over the logging on through a telecommunication network. Some systems have been proved to be vulnerable to shutting themselves down to prevent harm when they are overloaded. Hackers use this technique to shut down computer systems over the Internet.


Hacker
Hacker disrupts service provided by server
Internet Communication Facility
Mr. B
Server

Denial of Service

Question 13

Explain some of the key ways to control remote and distributed data processing applications in brief.

Answer

Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.
- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- In order to prevent unauthorized users from accessing the system, there should be proper control mechanisms over system documentation and manuals.

- Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations it must be ensured that all identical copies contain the same information and checks are also implemented to ensure that duplicate data does not exist.

Question 14

Discuss the three processes of Access Control Mechanism, when a user requests for resources.

Answer

An Access Control Mechanism is associated with identified, authorized users the resources they are allowed to access and action privileges. The mechanism processes the users request for Real time Memory and Virtual Memory resources in three steps:

- **Identification:** First and foremost, the users have to identify themselves.
- **Authentication:** Secondly, the users must authenticate themselves and the mechanism must authenticate itself. The mechanism accesses previously stored information about users, the resources they can access, and the action privileges they have with respect to these resources; it then permits or denies the request. Users may provide four factor of authentication information as described in Table below:

Classes of Authentication

Remembered information	Name, Account number, passwords
Objects Possessed by the user	Badge, plastic card, key
Personal characteristics	Finger print, voice print, signature
Dialog	Through/around computer

- **Authorization:** Third, the users request for specific resources, their need for those resources and their areas of usage of these resources. There are two approaches to implementing the authorization module in an access control mechanism:
    - a “ticket oriented approach”, and
    - a “list oriented approach”.

  Considering the authorization function in terms of a matrix where rows represent the users and columns represent the resources and the element represents the users privilege on the resources, we can see the distinction between these two approaches.
- In a **ticket-oriented approach** to authorization, the access control mechanism assigns 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.

- In a **list-oriented 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. This mechanism operates via a column in the matrix.

Question 15

Discuss Locks on Doors with respect to physical access controls in brief.

Answer

Locks on Doors: 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, 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.
- **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 be not be duplicated.
- **Electronic Door Locks –** A magnetic or embedded chip-based plastics card key or token may be entered into a reader to gain access in these systems. The reader device reads the special code that is internally stored within the card activates the door locking mechanism.

Question 16

Discuss major dimensions under which the impact of cyber frauds on enterprises can be viewed.

Or

What are the repercussions of cyber frauds on an enterprise?

Answer

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- **Financial Loss:** Cyber frauds lead to actual cash loss to target company/organization. For example, wrongful 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 organization's database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to loss of credibility. There have been instances where share prices of such companies went down, when the news of such attach percolated to the market.
- **Disclosure of Confidential, Sensitive or Embarrassing Information:** Cyber-attack may expose critical information in public domain. For example, instances of individuals leaking information about government's secret programs.
- **Sabotage:** The above situation may lead to misuse of such information by enemy country.

Question 17

Discuss major techniques to commit cyber frauds in brief.

Answer

Following are the major techniques to commit cyber frauds:

- **Hacking:** It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
- **Cracking:** Crackers are hackers with malicious intentions, which means, intent to cause harm. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.
- **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 referred as data diddling.
- **Data Leakage:** It refers to the unauthorized copying of company data such as computer files.
- **Denial of Service (DoS) Attack:** It refers to an action or series of actions that prevents access to a system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
- **Internet Terrorism:** It refers to using the Internet to disrupt electronic commerce and to destroy company and individual communications.
- **Logic Time Bombs:** These are programs that lie idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- **Masquerading or Impersonation:** In this case, perpetrator gains access to the system by pretending to be an authorized user.
- **Password Cracking:** Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.

- **Piggybacking:** It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
- **Scavenging or Dumpster Diving:** It refers to the gaining access to confidential information by searching discarded corporate records.
- **Social Engineering Techniques:** In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
- **Super Zapping:** It refers to the unauthorized use of special system programs to bypass regular system controls and perform illegal acts.
- **Trap Door:** In this technique, perpetrator enters into the system using a back door that bypasses normal system controls and perpetrates fraud.

Question 18

Discuss any three Internetworking devices.

Answer

Device	Functions
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 are 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.

Question 19

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.

Answer

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.

Major Boundary Control techniques are as follows:

- *Cryptography: It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. Techniques of cryptography are Transposition, Substitution and Product Cipher.*
- *Passwords: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.*
- *Personal Identification Numbers (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.*
- *Identification Cards: Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.*
- *Biometric Devices: Biometric identification e.g. thumbs and/or finger impression, eye retina etc. are also used as boundary control techniques.*

Question 20

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.

Answer

Risks related to the use of PCs in the business are as follows:

- *Personal computers are small in size and easy to connect and disconnect, they are likely to be shifted from one location to another or even taken outside the organization for theft of information.*
- *Pen drives can be very conveniently transported from one place to another, as a result of which data theft may occur. Even hard disks can be ported easily these days.*

- *PC is basically a single user oriented machine and hence, does not provide inherent data safeguards. Problems can be caused by computer viruses and pirated software, namely, data corruption, slow operations and system break down etc.*
- *Segregation of duty is not possible, owing to limited number of staff.*
- *Due to vast number of installations, the staff mobility is higher and hence becomes a source of leakage of information.*
- *The operating staff may not be adequately trained.*
- *Weak access control: Most of the log-on procedures become active at the booting of the computer from the hard drive.*

The Security Measures that could be exercised to overcome these aforementioned risks are given as follows:

- *Physically locking the system;*
- *Proper logging of equipment shifting must be done;*
- *Centralized purchase of hardware and software;*
- *Standards set for developing, testing and documenting;*
- *Uses of antimalware software; and*
- *The use of personal computer and their peripheral must have controls.*
- *Use of disc locks that prevent unauthorized access to floppy disk or pen drive of a computer.*

Question 21

As an IS auditor, what are the output controls required to be reviewed with respect to application controls?

Answer

As an IS Auditor, various Output Controls required to be reviewed with respect to Application Controls are as follows:

- *Storage and logging of sensitive, critical forms: Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.*
- *Logging of output program executions: When programs used for output of data are executed, these should be logged and monitored; otherwise on confidentiality/ integrity of the data may be compromised.*
- *Spooling/queuing: "Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user is able to continue working, while the print operation is getting completed.*

- *Controls 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.*
- *Report distribution and collection controls:* *Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. A log should be maintained for reports that were generated and to whom these were distributed. Uncollected reports should be stored securely.*
- *Retention controls:* *Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced.*

Question 22

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.

Answer

User Controls: *Application system represents the interface between the user and the business functions. From the users' perspective, it is the applications that drive the business logic and thus User Controls are required. The user controls that are to be exercised for system effectiveness and efficiency are as follows:*

- *Boundary Controls:* *These establish interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Further users are allowed using resources in restricted ways.*
- *Input Controls:* *Responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input Controls are validation and error detection of data input into the system.*
- *Processing Controls:* *These controls are responsible for computing, sorting, classifying and summarizing data. These maintain the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.*
- *Output Controls:* *These controls provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.*
- *Database Controls:* *These are responsible to provide functions to define, create, modify, delete and read data in an information system. These maintain procedural data-set of rules to perform operations on the data to help a manager to take decisions.*

Question 23

Do you consider Corrective Controls are a part of Internal Controls? Describe the characteristics of Corrective Controls.

Answer

Yes, we consider Corrective Controls to be a part of Internal Controls. Corrective controls are designed to reduce the impact or correct an error once it has been detected. Contingency planning, Backup procedure, Rerun procedures, and Investigate budget variance and report violations are some of the examples of corrective controls. The main characteristics of the corrective controls are as follows:

- ***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.***

Exercise

1. *Discuss major General Controls within an enterprise in brief.*
2. *What do you mean by Detective Controls? Explain with the help of examples. Also describe their main characteristics in brief.*
3. *Discuss Application Controls and their categories in brief.*
4. *'There are various general guidelines, with reference to 'Segregation of Duties', which may be followed in addition with the concepts like, 'maker should not be the checker'. Explain those guidelines.*
5. *What is 'Data Integrity'? Explain six categories of Integrity Controls in brief.*
6. *Explain some of the key logical access controls in detail with the help of suitable examples.*
7. *Describe major controls over environmental exposures.*
8. *What is Cyber Fraud? Differentiate between pure cyber frauds and cyber enabled frauds.*
9. *Explain major cyber-attacks reported by various agencies in recent years.*
10. *Discuss Managerial Controls and their categories in brief.*
11. *Write short notes on the following:*

    (i) Need for protection of Information Systems

    (ii) Compensatory Controls

    (iii) BCP Controls

    (iv) Cyber Frauds

    (v) Topological Controls

    (vi) Backup Controls

4

Business Continuity Planning and Disaster Recovery Planning

Basic Concepts

1. **Business Continuity Management:** Business Continuity means maintaining the uninterrupted availability of all key business resources required to support essential business activities. Key terms relating to BCM are:

- **Business Contingency:** A business contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.
- **BCP Process:** BCP is a process designed to reduce the risk to an enterprise from an unexpected disruption of its critical functions, both manual and automated ones, and assure continuity of minimum level of services necessary for critical operations.
- **Business Continuity Planning (BCP):** It refers to the ability of enterprises to recover from a disaster and continue operations with least impact.

2. **BCP Manual:** A BCP manual is a documented description of actions to be taken, resources to be used and procedures to be followed before, during and after an event that severely disrupts all or part of the business operations.

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

4. Business Continuity Planning: Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an enterprise will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business continuity covers the following areas:

- **Business Resumption Planning:** This is the operation's piece of business continuity planning.
- **Disaster Recovery Planning<** This is the technological aspect of business continuity planning, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of disaster.
- **Crisis Management:** This is the overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

5. Objectives of Business Continuity Planning: The primary objective of a business continuity plan is to minimize loss by minimizing the cost associated with disruptions and enable an organization to survive a disaster and to re-establish normal business operations. In order to survive, an organization must assure that critical operations can resume normal processing within a reasonable time frame.

6. Developing a Business Continuity Plan: The methodology for developing a business continuity plan can be sub-divided into eight different phases: Pre-Planning Activities (Business continuity plan Initiation), Vulnerability Assessment and General Definition of Requirements, Business Impact Analysis, Detailed Definition of Requirements, Plan Development, Testing Program, Maintenance Program, Initial Plan Testing and Plan Implementation.

7. Components of BCM Process: Components of BCM Process are shown in the Fig. 4.1:

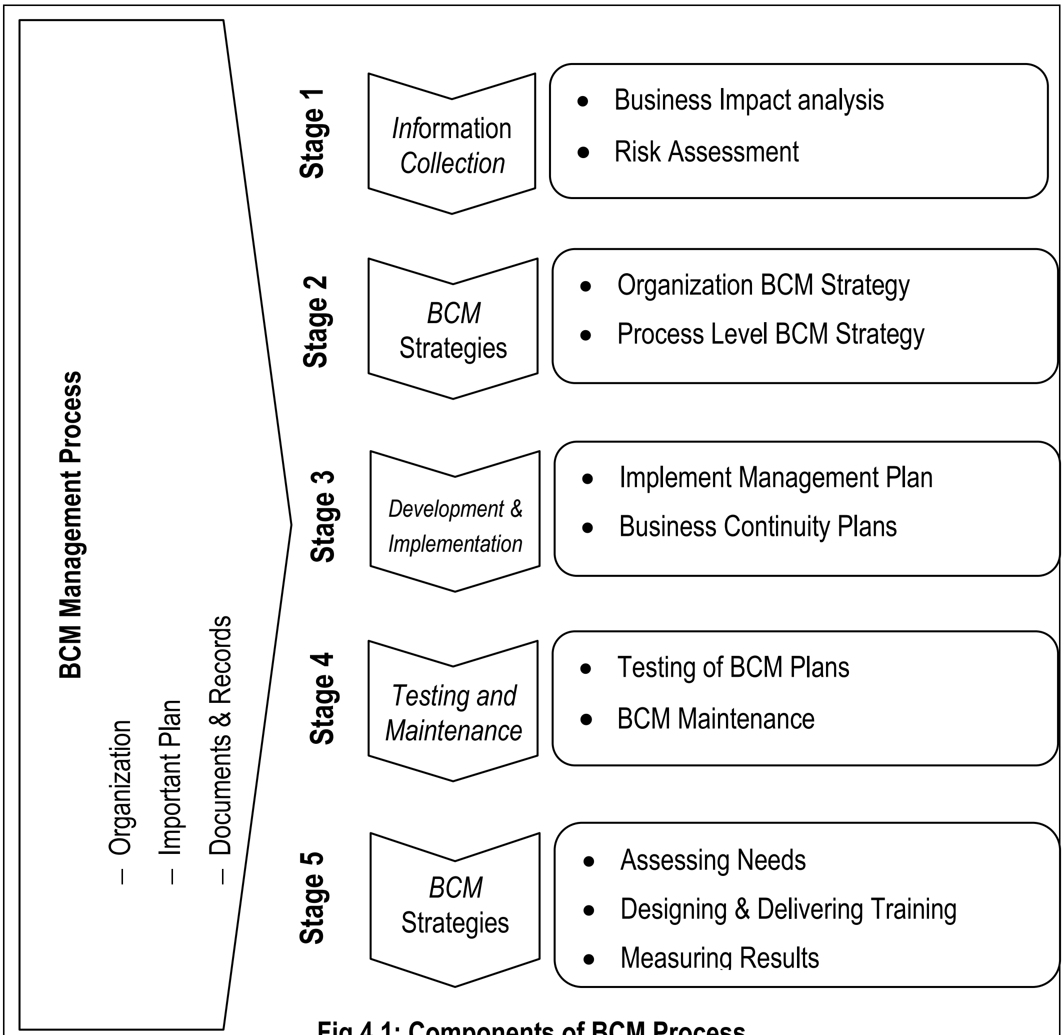


Fig 4.1: Components of BCM Process

8. BCM Management Process: A BCM process should be in place to address the policy and objectives as defined in the business continuity policy by providing organization structure with responsibilities and authority, implementation and maintenance of business continuity management.

9. BCM Information Collection Process: The pre-planning phase of Developing the BCP also involves collection of information. It enables the organization to define the scope of BCP and the associated work program; develop schedules; and identify and address issues that could have an impact on the delivery and the success of the plan. Two other key deliverables of that phase are: the development of a policy to support the recovery programs; and an awareness program to educate management and senior individuals who will be required to participate in the business continuity program.

Business Impact Analysis: Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

10. BCM Strategy Process: Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications.

The enterprise develops and documents a series of plans, which enable them to effectively manage an incident, which impacts on site operations and subsequently recover its critical activities and their supporting resources, within the timescales agreed with the customer.

11. BCM Development and Implementation Process: The enterprise should have an exclusive organization structure, Incident Management Team / Crisis management team for an effective response and recovery from disruptions.

12. BCM Testing and Maintenance Process: A BCP has to be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become outdated as time passes and as the resources used to support critical functions change. Responsibility for keeping the plan updated has to be clearly defined in the BCP. A BCM testing should be consistent with the scope of the BCP(s), giving due regard to any relevant legislation and regulation. Testing may be based on a predetermined outcome, (e.g. plan and scope in advance) or allow the enterprise to develop innovative solutions.

The BCM maintenance process demonstrates the documented evidence of the proactive management and governance of the enterprise's business continuity program; that the key people who are to implement the BCM strategy and plans are trained and competent; the monitoring and control of the BCM risks faced by the enterprise; and the evidence that material changes to the enterprise's structure, products and services, activities, purpose, staff and objectives have been incorporated into the enterprise's business continuity and incident management plans.

13. Types of Plans: Various plans are as under:

- **Emergency Plan:** The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs.
- **Back-up Plan:** The backup plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting

operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system.

- **Recovery Plan:** The backup plan is intended to restore operations quickly so that information system functions can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first.
- **Test Plan:** The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to assure that the DR plan will work and to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. Periodically, test plans must be invoked.

14. Types of Back-ups: Various types of back-ups are given as follows**:**

- **Full Backup:** A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes, prevents it from being a realistic proposition for backing up a large amount of data.
- **Incremental Backup:** An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.
- **Differential Backup:** A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.
- **Mirror back-up:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

15. Alternate Processing Facility Arrangements: Security administrators should consider the following backup options:

- **Cold site:** If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a system-raised floors, air conditioning, power, communication lines, and so on.
- **Hot site:** If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain.

- **Warm site:** A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the 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:** Two or more organisations 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.

16. Audit of the BCP/DRP: In a BCP Audit, the auditor is expected to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption. The objective of BCP audit is to assess the ability of the enterprise to continue all critical operations during a contingency and recover from a disaster within the defined critical recover time period. BCP Auditor is expected to identify residual risks, which were not identified and provide recommendations to mitigate them. The plan of action for each type of expected contingency and its adequacy in meeting contingency requirements is also assessed in a BCP audit.

Question 1

Discuss the objectives of Business Continuity planning.

Answer

Objectives of Business Continuity Planning: 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:

- Provide for the safety and well-being of people on the premises at the time of disaster;
- Continue critical business operations;
- Minimise the duration of a serious disruption to operations and resources (both information processing and other resources);
- Minimise immediate damage and losses;
- Establish management succession and emergency powers;
- Facilitate effective co-ordination of recovery tasks;
- Reduce the complexity of the recovery effort;
- Identify critical lines of business and supporting functions.

Question 2

Describe the methodology of developing a Business Continuity Plan. Also enumerate its eight phases.

Answer

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:

(i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;

(ii) Obtaining commitment from appropriate management to support and participate in the effort;

(iii) Defining recovery requirements from the perspective of business functions;

(iv) Documenting the impact of an extended loss of availability to operations and key business functions;

(v) Focusing appropriately on disaster prevention and impact minimisation, as well as orderly recovery;

(vi) Selecting business continuity teams that ensure the proper balance required for plan development;

(vii) Developing a business continuity plan that is understandable, easy to use and maintain; and

(viii) Defining how business continuity considerations must be integrated into on-going business planning and system development processes in order that the plan remains viable over time.

The eight phases are given as follows:

(i) Pre-Planning Activities (Business Continuity Plan Initiation),

(ii) Vulnerability Assessment and General Definition of Requirements,

(iii) Business Impact Analysis,

(iv) Detailed Definition of Requirements,

(v) Plan Development,

(vi) Testing Program,

(vii) Maintenance Program, and

(viii) Initial Plan Testing and Plan Implementation.

Question 3

While developing a Business Continuity Plan, what are the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement'?

Answer

While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement' are given as follows:

- A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.
- The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- Define the scope of the planning effort.
- Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- Develop a Plan Framework.

Question 4

What are the major documents that should be the part of a Business Continuity Management system? Explain in brief.

Answer

All documents that are part of the BCM are subject to document control and record control processes. The following are the major documents, which should be the part of the business continuity management system:

- The business continuity policy;
- The business impact analysis report;
- The risk assessment report;
- The aims and objectives of each function;

- The activities undertaken by each function;
- The business continuity strategies;
- The overall and specific incident management plans;
- The business continuity plans;
- Change control, preventative action, corrective action, document control and record control processes;
- Local Authority Risk Register;
- Exercise schedule and results;
- Incident log; and
- Training program.

Question 5

Discuss the maintenance tasks undertaken in the development of a BCP in brief.

Answer

Major maintenance tasks undertaken in development of a BCP are to:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
- Identify the BCP maintenance triggers to ensure that any organizational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date;
- Determine the maintenance regime to ensure the plan remains up-to-date;
- Determine the maintenance processes to update the plan; and
- Implement version control procedures to ensure that the plan is maintained up-to-date.

Question 6

Briefly explain various types of system's back-up for the system and data together.

Or

Explain briefly data back-up techniques.

Answer

***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:**

***Full Backup:* A Full Backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the**

backup set. At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed. For example - Suppose a full backup job or task is to be done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders in the backup job. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not. The cycle continues this way.

Incremental Backup: An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup. For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full backup since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.

Differential Backup: Differential backups fall in the middle between full backups and incremental backup. A Differential Backup stores files that have changed since the last full backup. With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken. On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and files added since Monday's full backup will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on Tuesday.

Mirror back-up: Mirror backups are, as the name suggests, a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup. For example - Many online backup services offer a mirror backup with a 30 day delete. This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted. This helps strike a balance offering a level of safety while not allowing the backups to keep growing since online storage can be relatively expensive. Many backup software utilities do provide support for mirror backups.

Question 7

Explain briefly the following terms with respect to business continuity and disaster recovery planning.

(i) Emergency Plan

(ii) Recovery Plan

(iii) Test Plan

Answer

(i) Emergency plan: The emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situations that invoke the plan have been identified, four aspects of the emergency plan must be articulated. First, the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'. Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation procedures required must be specified. Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be defined. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

(ii) Recovery Plan: The backup plan is intended to restore operations quickly so that information system function can continue to service an organization, whereas, recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Members of a recovery committee must understand their responsibilities. Again, the problem is that they will be required to undertake unfamiliar tasks. Periodically, they must review and practice executing their responsibilities so they are prepared should a disaster occur. If committee members leave the organization, new members must be appointed immediately and briefed about their responsibilities.

(iii) Test Plan: The final component of a disaster recovery plan is a test plan. The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

Question 8

Explain briefly the following terms with respect to alternate processing facility arrangements in business continuity and disaster recovery planning.

(i) Cold Site

(ii) Hot Site

(iii) Warm Site

Answer

(i) Cold site: If an organisation can tolerate some downtime, cold-site backup might be appropriate. A cold site has all the facilities needed to install a system-raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.

(ii) Hot site: If fast recovery is critical, an organisation might need hot site backup. All hardware and operations facilities will be available at the hot 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 organisations that have hot-site needs.

(iii) Warm site: A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the 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.

Question 9

A company has decided to outsource its recovery process to a third party site. What are the issues that should be considered by the security administrators while drafting the contract?

Answer

If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover the following issues:

- How soon the site will be made available subsequent to a disaster;
- The number of organizations that will be allowed to use the site concurrently in the event of a 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 the site can be used;
- The facilities and services the site provider agrees to make available;
- Procedures to ensure security of company's data from being accessed/damaged by other users of the facility; and
- What controls will be in place for working at the off-site facility.

Question 10

Describe contents of a Disaster Recovery and Planning Document.

Answer

Disaster Recovery Procedural Plan Document: The disaster 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.

Question 11

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

Answer

An audit or self-assessment of the enterprise's BCM (Business Continuity Management) program 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.*

Question 12

Explain the objectives of Business Continuity Management Policy briefly.

Answer

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.*

Question 13

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

Answer

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 that have been 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.*

Question 14

Write short note on the following:

(a) Types of Backups

(b) Backup option sites for Alternate processing facility arrangements

Answer

(a) 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:

- *Full Backup: A full backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. However, the amount of time and space such a backup takes prevents it from being a realistic proposition for backing up a large amount of data.*
- *Incremental Backup: An incremental backup captures files that were created or changed since the last backup, regardless of backup type. This is the most economical method, as only the files that changed since the last backup are backed up. This saves a lot of backup time and space.*

  Normally, incremental backup are very difficult to restore. One will have to start with recovering the last full backup, and then recovering files, which were charged subsequently from every subsequent incremental backup.
- *Differential Backup: A differential backup stores files that have changed since the last full backup. Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full back up. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.*

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.

- ***Mirror back-up:** A mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.*

(b) Security administrators should consider the following Backup option sites for alternate processing facility arrangements:

- ***Cold site:** A cold site has all the facilities needed to install a mainframe system-raised floors, air conditioning, power, communication lines, and so on. An organisation can establish its own cold-site facility or enter into an agreement with another organisation to provide a cold-site facility.*
- ***Hot site:** All hardware and operations facilities will be available at the hot site. In some cases, software, data and supplies might also be stored there. A hot site is expensive to maintain and are usually shared with other organisations that have hot-site needs.*
- ***Warm site:** A warm site provides an intermediate level of backup. It has all cold-site facilities in addition to the hardware that might be difficult to obtain or install.*
- ***Reciprocal agreement:** Two or more organisations 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.*

Exercise

1. *Explain the objectives of performing BCP tests while developing a business continuity plan.*
2. *Briefly explain maintenance tasks undertaken in the development of a business continuity plan.*
3. *What are the key aspects that should be verified during audit/self-assessment of an enterprise' BCM program while reviewing BCM arrangements?*
4. *Differentiate between Incremental Backup and Differential Backup.*
5. *Write short notes on the following:*

   (i) BCP Manual *(ii) BCP Strategy Process*

   (iii) Back-up Plan *(iv) BCM Testing*

   (v) BCM Maintenance
6. *Differentiate between Cold Site and Hot Site.*

5

Acquisition, Development and Implementation of Information Systems

Basic Concepts

1. Business Process Design: Business Process Design means structuring or restructuring the tasks, functionalities and activities for improvising a business system. Business process design involves a sequence of steps, which are: *Present Process Documentation, Proposed Process Documentation and Implementation of New Process.*

2. System Development: It refers to the process of examining a business situation with the intent of improving it through better procedures and methods. System development can generally be thought of as having two major components:

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

3. Achieving System Development Objectives: Achieving the objectives of the system development is essential but many times, such objectives are not achieved as desired. An analysis on 'Why organizations fail to achieve their systems development objectives' reveals bottlenecks. Some of the most notable ones are given as follows:

(i) **User Related Issues:** It refers to those issues where user/customer is reckoned as the primary agent. Some of the aspects with regard to this problem are: *Shifting User Needs, Resistance to Change, Lack of User Participation, Inadequate Testing and User Training.*

(ii) **Developer Related Issues**: It refers to the issues and challenges with regard to the developers. Some of the critical bottlenecks are: *Lack of Standard Project Management and System Development Methodologies, Overworked or Under-Trained Development Staff.*

(iii) **Management Related Issues:** It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals. Some of such bottlenecks are: *Lack of Senior Management Support and Involvement, Non-development of Strategic Systems*.

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

4. **Accountants' Involvement in Development Work:** An accountant can help in various related aspects during system development; some of them are as follows:

(i) **Return on Investment (referred as RoI):** This defines the return, an entity shall earn on a particular investment i.e. capital expenditure. For this analysis, following data needs to be generated.

(a) **Cost:** This includes estimates for typical costs involved in the development, which are *Development Costs, Operating Costs, and Intangible Costs*.

(b) **Benefits:** The benefits, which result from developing new or improved information systems that can be subdivided into tangible and intangible benefits.

(ii) **Computing Cost of IT Implementation and Cost Benefit Analysis:** For analysis of RoI, accountants need the costs and returns from the system development efforts.

5. **Systems Development Methodology:** A System Development methodology is a formalized, standardized, well-organized and documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Major approaches are:

- **Waterfall Model:** This is a traditional development approach in which each phase is carried out in sequence or linear fashion. These phases include Requirements Analysis, Specifications and Design Requirements, Coding, Final Testing, and Release.
- **The Prototyping Model:** The goal of prototyping approach is to develop a small or pilot version called a Prototype of a 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 modifying/replicating/expanding or even replacing it by a full-scale and fully operational system. As users work with the prototype, they learn about the system criticalities and make suggestions about ways to manage it. These suggestions are then incorporated to improve the prototype, which is also used and evaluated. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or if it is not suitable (economically or functionally), it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.
- **The Incremental Model:** The Incremental model is a method of software development where the model is designed, implemented and tested incrementally (a little more is added each time) until the product is finished. The product is defined as finished when it satisfies all of its requirements. This model combines the elements of the waterfall model with the iterative philosophy of prototyping.
- **Spiral Model:** The Spiral model is a software development process combining elements of both design and prototyping-in-stages. It tries to combine advantages of top-down and bottom-up concepts. It combines the features of the prototyping model and the waterfall model. The spiral model is intended for large, expensive and complicated projects. Game

development is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects.

- **Rapid Application Development (RAD) Model:** Rapid Application Development (RAD) refers to a type of software development methodology, which uses minimal planning in favor of rapid prototyping. The planning of software developed using RAD is interleaved with writing the software itself. The lack of extensive pre-planning generally allows software to be written much faster, and makes it easier to change requirements.
- **Agile Model:** This is an organized set 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.

6. System Development Life Cycle (SDLC): SDLC provides system designers and developers to follow a sequence of activities. It consists of a generic sequence of steps or phases in which each phase of the SDLC uses the results of the previous one. These phases are given as under:

Table 5.1: System Development Life Cycle

S. No.	PHASE NAME	NATURE OF ACTIVITY
1.	Preliminary Investigation	Determining and evaluating the strategic feasibility of the system and ensure that the solution fits the business strategy.
2.	Systems Requirements Analysis	Analyzing the typical system requirements, in view of its functionalities, deliverables etc.
3.	Systems Design	Designing the system in terms of user interface, data storage and data processing functions on the basis of the requirement phase by developing the system flowcharts, system and data flow diagrams, screens and reports.
4.	Systems Acquisition	This involves acquisition of operating infrastructure including hardware, software and services.
5.	Systems Development	Developing the system as per the system designed to fulfill of requirements to the satisfaction of all stakeholders.
6.	Systems Testing	Requisite testing to ensure valid and reliable implementation.
7.	Systems Implementation	Operationalization of the developed system for acceptance by management and user before migration of the system to live environment and data conversion from legacy system to the new system.

8.	Post Implementation Review and Maintenance	Continuous evaluation of the system as it functions in the live environment and its updation / maintenance.

7. Preliminary Investigation: It is predominantly aimed to determine and analyze the strategic benefits in implementing the system through evaluation and quantification of - productivity gains; future cost avoidance; cost savings, and Intangible benefits like improvement in morale of employees. The deliverable of the preliminary investigation includes a report including feasibility study observations. Major activities are:

(i) Identification of Problem: The first step in an application development is to define the problem clearly and precisely, which is done only after the critical study of the existing system and several rounds of discussions with the user group.

(ii) Identification of Objectives: After the identification of the problem, it is easy to work out and precisely specify the objectives of the proposed solution.

(iii) Delineation of Scope: The scope of a solution defines its typical boundaries. It should be clear and comprehensible to the user management stating the extent and 'what will be addressed by the solution and what will not'. The typical scope determination may be performed on the following dimensions: *Functionality Requirements, Data to be Processed, Control Requirements, Performance Requirements, Constraints, Interfaces, and Reliability requirements.*

Two primary methods with the help of which scope of the project can be analyzed are: *Reviewing Internal Documents and Conducting Interviews*.

(iv) Feasibility Study: After possible solution options are identified, project feasibility i.e. the likelihood that these systems can be implemented in the organization is determined. The Feasibility Study of a system is evaluated under following dimensions: *Technical, Financial, Economic, Schedule/Time, Resources, Operational, Behavioral and Legal*

(v) Reporting Results to Management: After the analyst articulates the problem, defines it along with its scope, s/he provides one or more solution alternatives, estimates the cost and benefits of each alternative and reports these results to management.

8. System Requirements Analysis: This phase includes a thorough and detailed understanding of the current system, identification of the areas that need modification to solve the problem, determination of user/managerial requirements and to have fair idea about various systems development tools. Major deliverable is *Systems Requirements Specification (SRS).*

A generic set of process is described as follows:

(i) Fact Finding: Every system is built to meet some set of needs; for example, the need of the organization for lower operational costs, better information for managers, smooth operations for users or better levels of services to customers. Various fact-finding techniques/tools are: *Documents, Questionnaires, Interviews and Observation.*

(ii) Analysis of the Present System: Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates. The following areas should be studied in depth: *Reviewing Historical Aspects, Analyzing Inputs, Reviewing Data Files, Reviewing Methods, Procedures and Data Communications, Analyzing Outputs, Reviewing Internal Controls, Modeling the Existing System, Undertaking Overall Analysis of the Existing system*.

(iii) System Analysis of Proposed Systems: After a thorough analysis of each functional area of the present information system, the proposed system specifications must be clearly defined, which are determined from the desired objectives set forth at the first stage of the study.

(iv) System Development Tools: Many tools and techniques have been developed to improve current information systems and to develop new ones. Major tools used for system development specification or representations can be classified into four categories based on the systems features. These are: *System Components and Flows, User Interface, Data Attributes and Relationships, Detailed System Processes***.**

Some popular tools are: *Structured English, Flowcharts, Data Flow Diagrams, Decision Tree, Decision Table, CASE Tools, System Components Matrix, Data Dictionary, User Interface Layout and Forms*

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

(vi) Roles Involved in SDLC: A variety of tasks during the SDLC are performed by special teams/committees/individuals based on requisite expertise as well as skills. Some of the generic roles are: *Steering Committee, Project Manager, Project Leader, Systems Analyst / Business Analyst, Module Leader/Team Leader, Programmer/Developers, Database Administrator, Quality Assurance, Testers, Domain Specialist, IS Auditor.*

9. Systems Design: The key objective of this phase to design an Information System that best satisfies users/managerial requirements. Design phase documents/deliverables include a ‘blueprint’ for the design with the necessary specifications for hardware, software, people and data resources. Major activities are as follows:

(a) Architectural Design: Architectural design deals with the organization of applications in terms of hierarchy of modules and sub-modules. At this stage, we identify major modules; functions and scope of each module; interface features of each module; modules that each module can call directly or indirectly and Data received from / sent to / modified in other modules.

(b) Design of Data/Information flow: The design of the data and information flow is a major step in the conceptual design of the new system. In designing the data / information flow for the proposed system, inputs required are - existing data / information flows, problems with the present system, and objective of the new system.

(c) Design of Database: Design of the database involves determining its scope ranging from local to global structure. The scope is decided on the basis of interdependence among organizational units. The design of the database involves four major activities: *Conceptual Modeling, Data Modeling, Storage Structure Design and Physical Layout Design*

(d) User Interface Design: It involves determining the ways in which users will interact with a system. The points that need to be considered while designing the user interface are: *Source documents to capture raw data, hard-copy output reports, Screen layouts for dedicated source-document input, Inquiry screens for database interrogation, Graphic and color displays, and Requirements for special Input/Output device*.

(e) Physical Design: For the physical design, the logical design is transformed into units, which in turn can be decomposed further into implementation units such as programs and modules. During physical design, the primary concern of the auditor is effectiveness and efficiency issues.

(f) System's Operating Platform: In some cases, the new system requires an operating platform including hardware, network and system software not currently available in an organization.

10. System Acquisition: After a system is designed either partially or fully, the next phase of the systems development starts, which relates to the acquisition of operating infrastructure including hardware, software and services.

(a) Acquisition Standards: Management should establish acquisition standards that address the security and reliability issues as per current state-of-the art development standards.

(b) Acquiring Systems Components from Vendors: At the end of the design phase, the organization gets a reasonable idea of the types of hardware, software and services; it needs for the system being developed. The following considerations are valid for both acquisition of hardware and software: *Vendor Selection, Geographical Location of Vendor, Presentation by Selected Vendors, Evaluation of Users Feedback*.

(c) Other Acquisition Aspects and Practices: In addition to the above, there are several other acquisition aspects and practices also, which are: *Hardware Acquisition, Software Acquisition, Contracts, Software Licenses and Copyright Violations, Validation of Vendors' proposals, Methods of Validating the proposal like Checklists, Point-Scoring Analysis, Public Evaluation Reports, Benchmarking Problems related to Vendor's Solutions, Testing Problems.*

11. System Development: This phase is supposed to convert the design specifications into a functional system under the planned operating system environment. Application programs are written, tested and documented, and system testing conducting. Finally, it results into a fully functional and documented system. A good coded application and programs should have the following characteristics: *Reliability, Robustness, Accuracy, Efficiency, Usability and Readability.*

Other related aspects of this phase are as follows:

(a) **Program Coding Standards:** The logic of the program outlined in the flowcharts is converted into program statements or instructions at this stage. For each language, there are specific rules concerning format and syntax.

(b) **Programming Language:** Application programs are coded in the form of statements or instructions and the same is converted by the compiler to object code for the computer to understand and execute.

(c) **Program Debugging:** Debugging refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compilation means that the program can be successfully converted from the source code written by the programmer into machine language instructions. For example, bugs may also arise when the program processes data (e.g. invalid input) resulting in abrupt terminations or errors. These will not be identified when computing.

(d) **Testing the Programs:** A careful and thorough testing of each program is imperative to successful installation of any system. The programmer should plan the testing to be performed, including testing of all possible exceptions.

(e) **Program Documentation:** Writing of narrative procedures and instructions for people, who will use software is done throughout the program life cycle. Managers and users should carefully review both internal and external documentation in order to ensure that the software and system behave as the documentation indicates.

(f) **Program Maintenance:** The requirements of business data processing applications are subject to periodic change. This calls for modification of various programs. There are usually separate categories of programmers called maintenance programmers, who are entrusted with this task.

12. System Testing: Testing is a process used to identify the correctness, completeness and quality of developed computer software. Different levels/facets of Testing are given as under:

(i) **Unit Testing:** 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. There are five categories of tests that a programmer typically performs on a program unit, which are:

- **Functional Tests:** Functional Tests check 'Whether programs do, what they are supposed to do or not'.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, throughput, primary and secondary memory utilization traffic rates on data channels and communication links.

- **Stress Tests:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

In terms of techniques, Unit Testing is classified as Static Analysis Testing and Dynamic Testing. Such typical testing techniques are:

(a) Static Testing: Static Analysis Tests are conducted on source programs and do not normally require executions in operating conditions. Typical static analysis techniques include: Desk Check, Structured Walk Through and Code Inspection.

(b) Dynamic Analysis Testing: Such testing is normally conducted through execution of programs in operating conditions. Typical techniques for dynamic testing and analysis include:

- **Black Box Testing:** Black Box Testing takes an external perspective of the test object, to derive test cases. These tests can be functional or non-functional, though they are usually functional.
- **White Box Testing:** It uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software.
- **Gray Box Testing:** It is a software testing technique that uses a combination of black box testing and white box testing.

(ii) Integration Testing: Integration testing is an activity of software testing in which individual software modules are combined and tested as a group. This is carried out in the following two manners:

- **Bottom-up Integration:** It is the traditional strategy used to integrate the components of a software system into a functioning whole. It consists of unit testing, followed by sub-system testing, and then testing of the entire system.
- **Top-down Integration:** It starts with the main routine, and stubs are substituted, for the modules directly subordinate to the main module.

(iii) Regression Testing: In the context of the integration testing, the regression tests ensure that changes or corrections have not introduced new faults. The data used for the regression tests should be the same as the data used in the original test.

(iv) System Testing: It is a process in which software and other system elements are tested as a whole. System testing begins either when the software as a whole is operational or when the well-defined subsets of the software's functionality have been implemented. The types of testing that might be carried out are:

- **Recovery Testing:** This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'.
- **Security Testing:** This is the process to determine whether an Information System protects data and maintains functionality as intended or not.
- **Stress or Volume Testing:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.
- **Performance Testing:** Performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.

(v) Final Acceptance Testing: It is conducted when the system is just ready for implementation. During this testing, it is ensured that the new system satisfies the quality standards adopted by the business and satisfies users. Thus, final acceptance testing has two major parts:

- **Quality Assurance Testing:** It ensures that the new system satisfies the prescribed quality standards and the development process is as per the organization's quality assurance policy, methodology and prescriptions.
- **User Acceptance Testing:** It ensures that functional aspects expected by users have been well addressed in the new system. There are two types of user acceptance testing: *Alpha Testing and Beta Testing*.

13. 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 Systems Implementation. Some of the generic activities involved in system implementation stage are:

(i) Equipment Installation: The hardware required to support the new system is selected prior to the implementation phase. Major tasks are: *Site Preparation, Installation of New Hardware / Software and Equipment Checkout*.

(ii) Training Personnel: Training is a major component of systems implementation. When a new system is acquired, which often involves new hardware and software, both users and computer professionals generally need some type of training.

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

- **Direct Implementation / Abrupt Change-Over:** 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 Changeover:** 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 a single operation but only on a small scale e.g. in one division. 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 the most 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.

(iv) System technical changeover or Conversion activities include *Procedure Conversion, File Conversion, System conversion and Scheduling Personnel and Equipment.*

14. Post Implementation Review: A Post Implementation Review answers the question “Did we achieve what we set out to do in business terms?” Typical evaluations include the following: *Development Evaluation, Operational Evaluation and Information Evaluation*.

15. System Maintenance: Maintaining the system is an important aspect of SDLC. Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for insuring operational continuity and avoidance of anticipated risks.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found during execution.
- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the 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 with the activities aimed at increasing the system’s maintainability, such as updating documentation, adding comments, and improving the modular structure of the system.

16. Operation Manuals: It is typical user’s guide, also commonly known as Operations Manual. Moreover, it may be a technical communication document intended to give assistance to people using a particular system.

Question 1

Discuss the key characteristics of Waterfall Model in brief. Also explain its major weaknesses.

Answer

Key characteristics of Waterfall Model are given as follows:

- Project is divided into sequential phases, with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

Though it is a highly useful model but it suffers from various weaknesses too. Experts and practitioners identify a number of weaknesses including the following:

- It is criticized to be Inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- Project progresses forward, with only slight movement backward.
- There is a little to iterate, which may be essential in some situations.
- It depends upon early identification and specification of requirements, even if the users may not be able to clearly define 'what they need early in the project'.
- Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
- Problems are often not discovered until system testing.
- System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- It is difficult to respond to changes, which may occur later in the life cycle, and if undertaken it proves costly and are thus discouraged.
- It leads to excessive documentation, whose updation to assure integrity is an uphill task and often time-consuming.
- Written specifications are often difficult for users to read and thoroughly appreciate.
- It promotes gap between users and developers with clear division of responsibility.

Question 2

Briefly explain Prototyping approach.

Answer

Prototyping approach: This approach is basically used for development of such systems 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 component that is built quickly and at a lesser cost, and with the intention of being modified or replacing it by a full-scale and fully operational system. As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporated into another prototype, which is also used and evaluated and so on. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or if it is not suitable. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

Experimenting with the prototype helps users to identify additional requirements and needs that they might have overlooked or forgotten to mention. In addition, with prototyping, users have a clearer visual picture of what the final version will look like and they do not have to sign off on a system, which is presented to them in the form of diagrams and specifications lists.

Question 3

Describe major strengths of Prototyping model.

Answer

Major strengths of prototyping model are given as follows:

- It improves both user participation in system development and communication among project stakeholders.
- It is especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
- Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
- It helps to easily identify, confusing or difficult functions and missing functionality.
- It enables to generate specifications for a production application.
- It encourages innovation and flexible designs.
- It provides for quick implementation of an incomplete, but functional, application.
- It typically results in a better definition of users' needs and requirements than traditional systems development approach.
- A very short time period is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.

- 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 traditional systems development approach is employed.

Question 4

Explain major strengths and weaknesses of Spiral model.

Answer

Major strengths of Spiral model are given as follows:

- It enhances risk avoidance.
- It is useful in helping for optimal development of a given software withiterations based on project risk.
- It can incorporate Waterfall, Prototyping, and Incremental methodologies as special cases in the framework, and provide guidance as to which combination of these models best fits a given software iteration, based upon the type of project risk. For example, a project with low risk of not meeting user requirements but high risk of missing budget or schedule targets would essentially follow a linear Waterfall approach for a given software iteration. Conversely, if the risk factors were reversed, the Spiral methodology could yield an iterative prototyping approach.

Major weaknesses of Spiral model are given as follows:

- It is challenging to determine the exact composition of development methodologies to use for each iteration around the Spiral.
- It may prove highly customized to each project, and thus is quite complex and limits reusability.
- A skilled and experienced project manager is required to determine how to apply it to any given project.
- No established controls exist for moving from one cycle to another cycle. Without controls, each cycle may generate more work for the next cycle.
- There are no firm deadlines, cycles continue with no clear termination condition leading to inherent risk of not meeting budget or schedule.

Question 5

What do you understand by agile model of software development? Also explain its major strengths and weaknesses in brief.

Answer

Agile Model: This is an organized set 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.

Strengths: Major strengths of agile model identified by the experts and practitioners include the following:

- Agile methodology has the concept of an adaptive team, which enables to respond to changing requirements.
- The team does not have to invest time and efforts and finally find that by the time they delivered the product, the requirement of the customer has changed.
- Face to face communication and continuous inputs from customer representative leaves little space for guesswork.
- The documentation is crisp and to the point to save time.
- The end result is generally the high quality software in least possible time duration and satisfied customer.

Weaknesses: Major weaknesses identified by the experts and practitioners include the following:

- In case of some software deliverables, especially large ones, it is difficult to assess the efforts required at the beginning of the software development life cycle.
- There is lack of emphasis on necessary designing and documentation.
- Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.
- Agile requires more re-work and due to lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.
- The project can easily get taken off track if the customer representative is not clear about the final outcome.
- Agile lacks attention to outside integration.

Question 6

State and briefly explain the stages of System Development Life Cycle (SDLC).

Answer

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.

Question 7

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 feasibility study of the system is to be conducted.

Answer

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.

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?

Some of the technical issues to be considered are given in the following table:

Table: Technical Issues

Design Considerations	Design Alternatives
Communications Channel configuration	Point to point, multidrop, or line sharing
Communications Channel	Telephone lines, coaxial cable, fiber optics, microwave, or satellite
Communications network	Centralized, decentralized, distributed, or local area
Computer programs	Independent vendor or in-house
Data storage medium	Tape, floppy disk, hard disk, or hard copy
Data storage structure	Files or database
File organization and access	Direct access or sequential files
Input medium	Keying, OCR, MICR, POS, EDI, or voice recognition
Operations	In-house or outsourcing
Output frequency	Instantaneous, hourly, daily, weekly, or monthly
Output medium	CRT, hard copy, voice, or turn-around document
Output scheduling	Pre-determined times or on demand
Printed output	Pre-printed forms or system-generated forms
Processor	Micro, mini, or mainframe
Transaction processing	Batch or online
Update frequency	Instantaneous, hourly, daily, weekly, or monthly

Due to tremendous advancements in computer field, the technology is available for most business data processing systems but sometimes not within the constraints of the firm's resources or its implementation schedule. Therefore, tradeoffs are often necessary. A technically feasible system may not be economically feasible or may be so sophisticated that the firm's personnel cannot effectively operate it.

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?

Question 8

What are the possible advantages of SDLC from the perspective of IS Audit?

Answer

From the perspective of the IS Audit, following are the possible advantages of SDLC:

- The IS auditor can have clear understanding of various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his/her examination, can state in his/her report about the compliance by the IS management with the procedures, if any, set by management.

- If the IS Auditor has technical knowledge and ability to handle different areas of SDLC, s/he can be a guide during the various phases of SDLC.
- The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

Question 9

What are the major aspects that need to be kept in mind while eliciting information to delineate scope?

Answer

Major aspects that need to be kept in mind while eliciting information to delineate scope are given as follows:

- Different users may represent the problem and required solution in different ways. The system developer should elicit the need from the initiator of the project (alternately called champion or executive sponsor of the project). Addressing his concerns should be the basis of the scope.
- While the initiator of the project may be a member of the senior management, the actual users may be from the operating levels in an organization. An understanding of their profile helps in designing appropriate user interface features.
- While presenting the proposed solution for a problem, the development organization has to clearly quantify the economic benefits to the user organization. The information required has to be gathered at this stage. For example, when a system is proposed for Road tax collection, data on the extent of collection and defaults is required to quantify benefits that will result to the Transport Department.
- It is also necessary to understand the impact of the solution on the organization- its structure, roles and responsibilities. Solutions, which have a wide impact, are likely to be met with greater resistance. ERP implementation in organizations is a classic example of change management requirement. Organizations that have not been able to handle it may have a very poor ERP implementation record with disastrous consequences.
- While economic benefit is a critical consideration when deciding on a solution, there are several other factors that have to be given weightage too. These factors are to be considered from the perspective of user management and resolved. For example, in a security system, how foolproof it is, may be a critical factor.

Question 10

Discuss in detail, how the analysis of present system is made by the system analyst?

Or

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.*

Answer

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.

The following areas may be studied in depth:

- **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 various 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 □ine 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.

Question 11

Explain two primary methods, which are used for the analysis of the scope of a project in SDLC.

Answer

Two primary methods, which are used for the analysis of the scope of a project in SDLC are given as follows:

- **Reviewing Internal Documents:** The analysts conducting the investigation first try to learn about the organization involved in, or affected by, the project. For example, to review an inventory system proposal, an analyst may try to know how the inventory department operates and who are the managers and supervisors. Analysts can usually learn these details by examining organization charts and studying written operating procedures.
- **Conducting Interviews:** Written documents tell the analyst how the systems should operate, but they may not include enough details to allow a decision to be made about the merits of a systems proposal, nor do they present users' views about current operations. To learn these details, analysts use interviews. Interviews allow analysts to know more about the nature of the project request and the reasons for submitting it. Usually, preliminary investigation interviews involve only management and supervisory personnel.

Question 12

What are the major objectives of system requirements analysis phase in the SDLC?

Answer

Major objectives of system requirements analysis phase in the SDLC are given as follows:

- To identify and consult stake owners to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To model activities such as developing models to document Data Flow Diagrams, Entity-Relationship Diagrams; and

- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

Question 13

If you are the Project Manager of a Software Company with the responsibility for developing a break-through product, combining state of the art hardware and software; will you opt for prototyping as a process model for a product meant for the intensely competitive entertainment market?

Answer

Prototyping as a process model will be inappropriate and hence inadvisable for the following reasons:

- Prototyping requires user involvement. Here, users are consumers of the product who are diffused and may not be inclined to join in.
- When we try to test the product with the involvement of customers, confidential or critical information might get leaked to the competitors on our line of thinking. The element of surprise and also the opportunity to capture the market will be lost.
- Prototyping requires significant time for experimenting. Since the product is meant for the intensely competitive entertainment market, the project manager may not have that much time to experiment, and the competitor may capture the market by entering the market in advance.

Question 14

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

Answer

The major tools used for system development can be grouped into four categories based on the systems features each document has. These are:

- Components and flows of a system,
- User interface,
- Data attributes and relationships, and
- Detailed system process.

Each of these categories is briefly discussed below:

- **System components and flows**: For system analysts, these tools are helpful to document the data flow among the major resources and activities of an information system. System flow charts are typically used to show the flow of data media as they are processed by hardware devices and manual activities. A system component matrix provides a matrix framework to document the resources used, the activities performed and the information produced by information system. A data flow diagram uses a few simple symbols to illustrate the flow of data among external entities.

- **User interface**: Designing the interface between end users and the computer system is a major consideration of system analysts while designing the new system. Layout forms and screens are used to construct the formats and contents of input / output media and methods. Dialogue flow diagrams analyze the flow of dialogue between computers and people. They document the flows among different display screens generated by alternative end user responses to menus and prompts.
- **Data attributes and relationships**: These tools are helpful to define, catalogue and design the data resources in information systems. A data dictionary catalogs the description of attributes of all data elements and their relationship to each other as well as to external systems. Entity – relationship diagrams are also used to document the number and type of relationship among entities in a system. File layout forms document the type, size, and names of the data elements in a system. Grid charts help in identifying the use of each type of data element in input / output or storage media of a system.
- **Detailed system process:** These tools are used to help the programmer to develop detailed procedures and processes required in the design of a computer program. Decision trees and decision tables use a network or a tabular form to document the complex conditional logic involved in choosing among the information processing alternatives in a system. Structure charts document the purpose, structure and hierarchical relationships of the modules in a program.

Question 15

Bring out the reasons as to why organizations fail to achieve their Systems Development Objectives?

Answer

Following are the major reasons due to which organizations fail to achieve their system development objectives:

(i) **User Related Issues:** It refers to those issues where user/customer is reckoned as the primary agent. Some of the aspects with regard to this problem are mentioned as follows:

- **Shifting User Needs:** User requirements for IT are constantly changing. As these changes accelerate, there will be more requests for Information systems development and more development projects. When these changes occur during a development process, the development team faces the challenge of developing systems whose very purpose might change after the development process began.
- **Resistance to Change:** People have a natural tendency to resist change, and information systems development projects signal changes - often radical - in the workplace. When personnel perceive that the project will result in personnel cutbacks, threatened personnel will dig in their heels, and the development project

is doomed to failure.

- **Lack of User Participation:** Often users do not participate in the development stage because they are preoccupied with their existing work, or do not understand the benefits of the new system. User apathy 'I have nothing to gain if I participate' is also a reason.
- **Inadequate Testing and User Training:** Often systems are not tested due to lack of time and rush to introduce the new system or because problems were not envisaged at the development stage. Inadequate user training may be a result of poor project planning, or lack of training techniques, or because user management does not release personnel for training due to operational pressure.

(ii) **Developer Related Issues**: It refers to the issues and challenges with regard to developers. Some of the critical bottlenecks are mentioned as follows:

- **Lack of Standard Project Management and System Development Methodologies:** Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- **Overworked or Under-Trained Development Staff:** In many cases, system developers lack sufficient educational background and requisite state of the art skills. Furthermore, many companies do little to help their development personnel stay technically sound, and often a training plan and training budget do not exist.

(iii) **Management Related Issues:** It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals. Some of such bottlenecks are mentioned as follows:

- **Lack of Senior Management Support and Involvement:** Developers and users of information systems watch senior management to determine 'which systems development projects are important' and act accordingly by shifting their efforts away from any project, which is not receiving management attention. In addition, management may not allocate adequate resources, as well as budgetary control over use of resources, assigned to the project.
- **Development of Strategic Systems:** Because strategic decision making is unstructured, the requirements, specifications, and objectives for such development projects are difficult to define.

(iv) **New Technologies:** When an organization tries to create a competitive advantage by applying advance technologies, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the technology.

In order to overcome these aforementioned issues, organizations must execute a well-planned systems development process efficiently and effectively. Accordingly, a sound system development team is inevitable for project success.

Question 16

Discuss major characteristics of a good coded program in brief.

Answer

A good coded program should have the following characteristics:

- **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.

Question 17

What is Unit Testing? Explain five categories of tests that a programmer typically performs on a program unit.

Or

Testing a program unit is essential before implementing it. Name any four categories of test; a programmer typically performs on a programmable unit.

Answer

Unit Testing: 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:

- **Functional Tests:** Functional Tests check 'whether programs do, what they are supposed to do or not'. The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

Question 18

Explain the following testing techniques:

(i) Black Box Testing

(ii) White Box Testing

(iii) Gray Box Testing

Answer

(i) Black Box Testing: Black Box Testing takes an external perspective of the test object, to derive test cases. These tests can be functional or non-functional, though usually functional. The test engineer has no prior knowledge of the test object's internal structure. The test designer selects typical inputs including simple, extreme, valid and invalid input-cases and executes to obtain assurance or uncover errors.

This method of test design is applicable to all levels of software testing i.e. unit, integration, functional testing, system and acceptance. The higher the level, the box is bigger and more complex, and the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested. If a module performs a function, which it is not supposed to, the black box test may not identify it.

(ii) White Box Testing: It uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to select paths through the code and determines the appropriate outputs. It is applicable at the unit, integration and system levels of the testing process, it is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.

(iii) Gray Box Testing: It is a software testing technique that uses a combination of black box testing and white box testing. In gray box testing, the tester applies a limited number of test cases to the internal workings of the software under test. For the remaining part of the software one takes a black box approach in applying inputs to the software under test and observing the outputs.

Question 19

Explain different changeover strategies used for conversion from old system to new system.

Answer

Different changeover strategies used for conversion from old system to new system are given as follows:

- **Direct Implementation / Abrupt Change-Over:** 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. Fig 5.1 (i) depicts Direct Implementation, which usually takes place on a set date, often after a break in production or a holiday period so that time can be used to get the hardware and software for the new system installed without causing too much disruption.

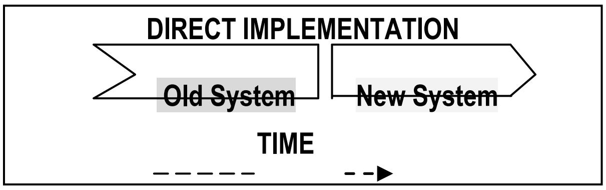


Fig. 5.1 (i): Direct Changeover

- **Phased Changeover:** With this strategy, implementation can be staged with conversion to the new system taking place gradually. For example, some new files may be converted and used by employees whilst other files continue to be used on the old system i.e. the new is brought in stages (phases). If a phase is successful then the next phase is started, eventually leading to the final phase when the new system fully replaces the old one as shown in Fig. 5.1(ii).

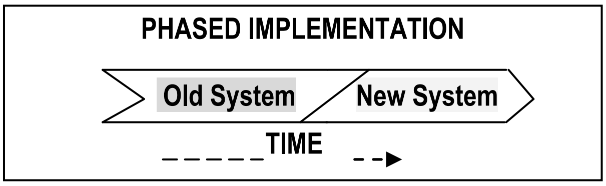


Fig. 5.1 (ii): Phased Changeover

- **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. For example - it might be tried out in one branch of the company or in one location. If successful the pilot is extended until it eventually replaces the old system completely. Fig. 5.1 (iii) depicts Pilot Implementation.

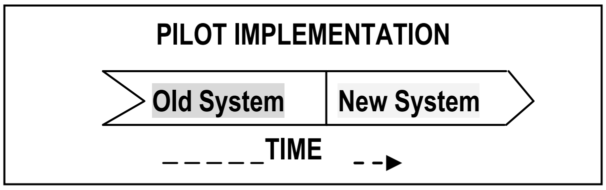


Fig. 5.1 (iii): Pilot Changeover

- **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. Fig. 5.1(iv) shows parallel implementation.

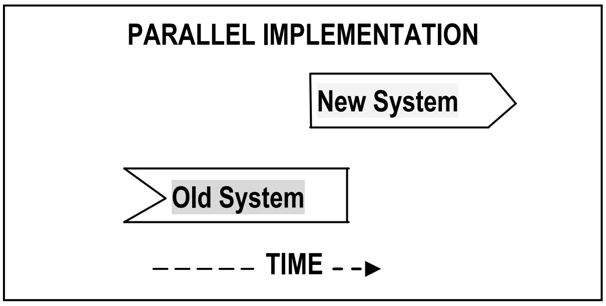


Fig. 5.1 (iv): Parallel Changeover

Question 20

Discuss briefly, various activities that are involved for successful conversion with respect to a computerized information system.

Answer

Activities involved in conversion: Conversion includes all those activities which must be completed to successfully convert from the existing manual system to the computerized information system. Fundamentally these activities can be classified as follows:

- Procedure conversion;
- File conversion;
- System conversion;
- Scheduling personnel and equipment; and
- Alternative plans in case of equipment failure.
- These are briefly discussed as follows:
- **Procedure 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 so 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 over come the unfavorable situation. Otherwise, panic will result in use of the least efficient methods when time is of the essence.

Question 21

Explain corrective and adaptive maintenance in brief.

Answer

Corrective Maintenance: Corrective maintenance deals with fixing bugs in the code or defects found during execution. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or correcting a failure to process the last record in a file.

Adaptive Maintenance: Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.

Question 22

Write short note on Design of database.

Answer

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.*

Question 23

Define the Agile model of software development and, discuss its strengths.

Answer

***Agile Methodology:** 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.*

Question 24

Many-a-time organizations fail to achieve their system development objectives. Justify the statement giving reasons.

Answer

Many-a-time organizations fail to achieve their systems development objectives. Some of the most notable reasons for this are as follows:

(i) *User Related Issues: It refers to those issues where user/customer is reckoned as the primary agent.*

- *Shifting User Needs: User requirements for IT are constantly changing and the development team faces the challenge of developing systems whose very purpose might change since the development process began.*
- *Resistance to Change: People have a natural tendency to resist change.*
- *Lack of User Participation: Users must participate in the development efforts to define their requirements, feel ownership for project success, and work to resolve development problems.*
- *Inadequate Testing and User Training: New systems must be tested before installation to determine that they operate correctly and users must be trained to effectively utilize the new system.*

(ii) *Developer Related Issues: It refers to the issues and challenges with regard to the developers.*

- *Lack of Standard Project Management and System Development Methodologies: Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.*
- *Overworked or Under-Trained Development Staff: In many cases, system*

developers often lack sufficient educational background and requisite state of the art skills.

(iii) ***<u>Management Related Issues:</u> It refers to the bottlenecks with regard to organizational set up, administrative and overall management to accomplish the system development goals.***

- ***<u>Lack of Senior Management Support and Involvement:</u> Senior management must provide guidance to developers and users of information systems in terms of which development projects are important so that they act accordingly.***
- ***<u>Development of Strategic Systems:</u> Because strategic decision making is unstructured; the requirements, specifications, and objectives for such development projects are difficult to define.***

(iv) ***<u>New Technologies:</u> When an organization tries to create a competitive advantage by applying advance technologies, it generally finds that attaining system development objectives is more difficult because personnel are not as familiar with the new technologies in practice. To obtain a required skill set in order to adapt new technologies becomes a major challenge for the organizations.***

Exercise

1. *What is waterfall model of system development? Also discuss its major strengths.*
2. *What is Rapid Application Development? Discuss its strengths and weaknesses in brief.*
3. *Agile methodology is one of the popular approaches of system development. What are the weaknesses of this methodology in your opinion?*
4. *What do you understand by feasibility study? Explain various types of feasibility studies in detail.*
5. *System Analysts use various fact-finding techniques for determining the needs/ requirements of a system to be developed. Explain these techniques in brief.*
6. *What do you understand by "Requirement analysis"? What is the significance of analyzing the present system and how is it carried out? Explain briefly.*
7. *What is SDLC? Explain the key activities performed in the Requirements Analysis phase.*
8. *Discuss the roles of the following with reference to SDLC:*

   (i) *Steering Committee*

   (ii) *System Analyst*

   (iii) *Database Administrator*

   (iv) *IS Auditor*
9. *Discuss Final Acceptance Testing in brief.*

10. *Write short notes on the following:*

    (i) Data Dictionary

    (ii) Static Testing

    (iii) Regression Testing

    (iv) System Testing

    (v) Preventive Maintenance

    (vi) Parallel Running Implementation

    (vii) Weaknesses of Incremental Model

    (viii) Auditors' involvement in development work

6

Auditing of Information Systems

Basic Concepts

1. Need for Audit of Information Systems: Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are depicted in the Fig. 6.1.

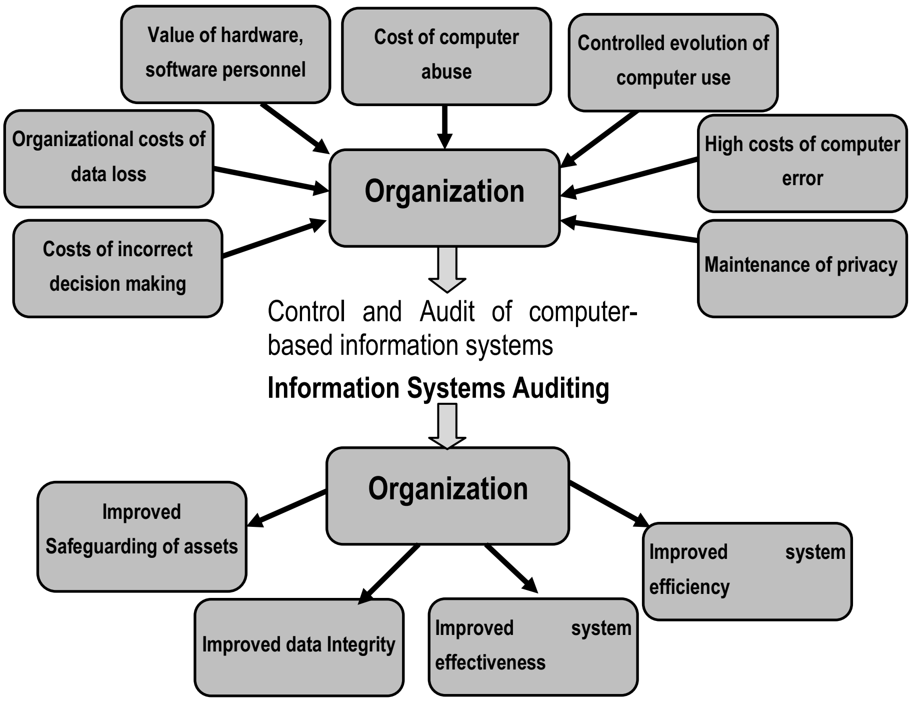

Value of hardware, software personnel
Cost of computer abuse
Controlled evolution of computer use
Organizational costs of data loss
Organization
High costs of computer error
Costs of incorrect decision making
Maintenance of privacy
Control and Audit of computer-based information systems
Information Systems Auditing
Organization
Improved Safeguarding of assets
Improved system efficiency
Improved data Integrity
Improved system effectiveness

Fig. 6.1: Impact of Controls and Auditing influencing an Organization

These are: *Organisational Costs of Data Loss, Incorrect Decision Making, Costs of Computer Abuse, Value of Computer Hardware, Software and Personnel*, *High Costs of Computer Error*, *Maintenance of Privacy, Controlled evolution of computer Use*, *Information Systems Auditing*, *Asset Safeguarding Objectives*, *Data Integrity Objectives*, *System Effectiveness Objectives* and *System Efficiency Objectives*.

2. Effect of Computers on Internal Audit: To cope up with the new technology usage in an enterprise, the auditor should be competent to provide independent evaluation as to whether the business process activities are recorded and reported according to established standards or criteria. Two basic functions carried out to examine these changes are:

(i) Changes to Evidence Collection: The performance of evidence collection and understanding the reliability of controls involves issues like- *Data retention and storage, Absence of input documents*, *Non-availability of audit trail, Lack of availability of output, Audit evidence* and *Legal issues*.

(ii) Changes to Evidence Evaluation: Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system. Major issues are: *System generated transactions, Automated transaction processin*g/generation *systems* and Systemic errors.

3. Responsibility for Controls: Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems.

4. IS Audit: The IS Audit of an Information System 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 information systems.
- Assessment of the efficiency and effectiveness of the IS environment.

5. Functions of IS Auditor: IS Auditors review risks relating to IT systems and processes; some of them are: *Inadequate information security controls , Inefficient use of resources, or poor governance , Ineffective IT strategies, policies and practices and IT-related frauds.*

6. Categories of IS Audits: IS Audits has been categorized into five types: *Systems and Application, Information Processing Facilities*, *Systems Development*, *Management of IT and Enterprise Architecture* and *Telecommunications, Intranets, and Extranets*.

7. Steps in Information System Audit: Different audit organizations go about IS auditing in different ways and individual auditors have their own favorite ways of working. However, it can be categorized into six stages, which are: *Scoping and pre-audit survey, Planning and preparation, Fieldwork, Analysis, Reporting and Closure.*

8. Audit Standards and Best Practices: These are: *IS auditing standards*, *IS auditing guidelines*, *IS auditing procedures & COBIT (Control objectives for information and related technology) of ISACA (Information Systems Audit and Control Association), ISO 27001, Internal Audit Standards, Standards on Internal Audit issued by ICAI and ITIL.*

9. Performing IS Audit: Various steps are given as follows:

(i) Basic Plan: Planning is one of the primary and important phase in an Information System Audit, which ensures that the audit is performed in an effective manner.

Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and that the work is completed expeditiously.

(ii) Preliminary Review: Some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review are: *Knowledge of the Business, Understanding the Technology, Understanding Internal Control Systems, Legal Considerations and Audit Standards and Risk Assessment and Materiality.* Risks are categorized as: *Inherent Risk, Control Risk and Detection Risk*.

10. Concurrent or Continuous Audit: Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the events at the client and the auditor's assurance services thereon. Continuous auditing techniques use two bases for collecting audit evidence. One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

Types of Audit Tools: Some of the well-known tools are:

(i) Snapshots: Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application.

(ii) Integrated Test Facility (ITF): The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness.

(iii) System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors might use SCARF to collect the different types of information such as *Application System Errors*, *Policy and Procedural Variances*, *System Exception*, *Statistical Sample*, *Snapshots and Extended Records*, *Profiling Data* and *Performance Measurement*.

(iv) Continuous and Intermittent Simulation (CIS): This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system.

Some of the advantages of continuous audit techniques are: *Timely, Comprehensive and Detailed Auditing*, *Surprise test capability*, *Information to system staff on meeting of objectives and Training for new users*.

(v) Audit Hooks: There are audit routines that flag suspicious transactions. For example, Internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

11. Audit Trail Objectives: Audit trails can be used to support security objectives in three ways: *Detecting unauthorized access to the system, Facilitating the reconstruction of events, and Promoting personal accountability.*

12. Role of IS Auditor in Physical Access Controls: Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves: *Risk Assessment*, *Controls Assessment* and *Review of Documents*.

13. Role of IS Auditor in Environmental Controls: Audit of environmental controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks. Documentation of Auditing of environmental controls activities is a critical part.

14. *Application Controls and their Audit Trail: These are categorized in the following types:*

- ***Boundary Controls: IT ensures that those who are using system are authentic users.***
- ***Input Controls: Responsible for bringing the data and instructions in to the information system.***
- ***Communication Controls: Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.***
- ***Processing Controls: Responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.***
- ***Database Controls: Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.***
- ***Output Controls: To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.***

15. Review of Controls at various Layers: For application security audit, a layered approach is used based on the functions and approach of each layer. This approach is in line with management structure, which follows top-down approach. Various layers are:

- **Operational Layer:** The basic layer, where user access decisions are generally put in place.
- **Tactical Layer:** The next is management layer, which includes supporting functions such as security administration, IT risk management and patch management.
- **Strategic Layer:** This is the layer used by top management. It includes the overall information security governance, security awareness, supporting information security policies and standards, and the overarching an application security perspective.

Various aspects relating to each aforementioned layer are given as follows:

- **Operational Layer:** The operational layer audit issues include: *User Accounts and Access Rights, Password Controls and Segregation of Duties.*
- **Tactical Layer**: At the tactical layer, security administration is put in place. This includes: *Timely updates to user profiles, like creating/deleting and changing of user accounts, IT Risk Management, Interface Security and Audit Logging and Monitoring.*
- **Strategic Layer:** At this layer, the top management takes action, in form of drawing up security policy, security training, security guideline and reporting. A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

  Based on the key controls described previously, the risk assessment of failure/weakness in the operating effectiveness of key application security controls shall be made and acted upon by auditor.

Question 1

Discuss the issues relating to the performance of evidence collection and understanding the reliability of controls.

Answer

The performance of evidence collection and understanding the reliability of controls involves the following major issues:

- **Data retention and storage:** A client’s storage capabilities may restrict the amount of historical data that can be retained “on-line” and readily accessible to the auditor. If the client has insufficient data retention capacities the auditor may not be able to review a whole reporting period transactions on the computer system. For example, the client’s computer system may save data on detachable storage device by summarizing transactions into monthly, weekly or period end balances.

- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of availability of output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output it may be necessary for the auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read-only" access to the required data files.
- **Audit evidence.** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalized) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- **Legal issues:** The use of computers to carry out trading activities is also increasing. More organizations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and who are the parties to the contract.

Question 2

Explain the set of skills that is generally expected of an IS auditor.

Answer

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

- Sound knowledge of business operations, practices and compliance requirements;
- Should possess the requisite professional technical qualification and certifications;
- A good understanding of information Risks and Controls;
- Knowledge of IT strategies, policy and procedural controls;

- Ability to understand technical and manual controls relating to business continuity; and
- Good knowledge of Professional Standards and Best Practices of IT controls and security.

Question 3

Explain major types of IS Audits in brief.

Answer

Major types of IS Audits are given as follows:

(i) **Systems and Application:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) **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.

(iii) **Systems Development:** An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

(iv) **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client (end point device), server, and on the network connecting the clients and servers.

Question 4

Explain major stages of IS Audits in brief.

Answer

Different audit organizations go about IS auditing in different ways and individual auditors have their own favourite ways of working. However, it can be categorized into the following major stages:

(i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

(ii) **Planning and preparation:** During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) **Fieldwork:** Gathering evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

(iv) **Analysis:** This step involves desperately sorting out, reviewing and trying to make sense of all the evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) **Reporting:** Reporting to the management is done after analysis of evidence gathered and analysed.

(vi) **Closure:** Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

Question 5

An important task for the auditor as a part of his/her preliminary evaluation is to gain a good understanding of the technology environment and related control issues. Explain major aspects that should be considered in this exercise.

Answer

Major aspects to be considered in the afore mention exercise are given as follows:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on Information Technology 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 architecture or a centralized architecture 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 and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems, and
- Finally, Studying Information Technology policies, standards, guidelines and procedures.

Question 6

What are the key steps that can be followed for a risk-based approach to make an audit plan? Explain in brief.

Answer

The steps that can be followed for a risk-based approach to make an audit plan are given as follows:

- Inventory the information systems 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 likelihood and severity of the impact on the business.
- Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Question 7

Write short notes on the following:

(i) Snapshots

(ii) Audit Hooks

(iii) Effect of Computers on Evidence Collection for audit

Answer

(i) Snapshots: Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

(ii) Audit Hooks: There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification may display a message on the auditor's terminal.

(iii) **Effects of Computers on Evidence Collection for Audit:** The performance of evidence collection and understanding the reliability of controls involves issues like -

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor due to which the auditor may not be able to review a whole reporting period transactions on the computer system.
- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation resulting in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time; thus making the auditor's job very difficult.
- **Lack of availability of printed output:** In the absence of physical output, it may be necessary for the auditor to directly access the electronic data retained on the client's computer.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system.
- **Legal issues:** Making use of Electronic Data Interchange (EDI) and electronic trading over the Internet can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.

Question 8

What do you understand by SCARF technique? Explain various types of information collected by using SCARF technique in brief.

Answer

System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written on a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Auditors might use SCARF technique to collect the following types of information:

- **Application System Errors -** 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 Variances -** 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 -** 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.
- **Statistical Sample -** 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.
- **Snapshots and Extended Records -** Snapshots and extended records can be written into the SCARF file and printed when required.
- **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.

Question 9

Describe major advantages of continuous audit techniques.

Answer

Major advantages of continuous audit techniques are given as follows:

- **Timely, Comprehensive and Detailed Auditing –** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability –** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives –** Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating

whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.

- **Training for new users –** Using the ITFs, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

Question 10

Describe major disadvantages and limitations of Continuous Audit techniques.

Answer

Major disadvantages and limitations of continuous audit techniques are given as follows:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

Question 11

Explain three major ways by which audit trails can be used to support security objectives.

Answer

Audit trails can be used to support security objectives in the following three ways:

- **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

Question 12

Discuss major audit issues of operational layer with reference to application security audit.

Answer

Major audit issues of operational layer with reference to application security audit are given as follows:

- **User Accounts and Access Rights:** This includes 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, and these need to be traceable to individuals for whom they are created. In case, guest IDs are used, then these should be tested. Likewise, vendor accounts and third-party accounts should be reviewed. In essence, users and applications should be uniquely identifiable.
- **Password Controls:** In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum. Auditor needs to check whether there are applications where password controls are weak. In case such instances are found, then auditor may look for compensating controls against such issues.
- **Segregation of Duties:** As frauds due to lack of segregations increase across the world, importance of the Segregation of Duties also increases. As defined earlier, Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to the responsibility for initiating and recording transactions and custody of assets to separate individuals. Example to illustrate:
    - Record keeper of asset must not be asset keeper.
    - Cashier who creates a cash voucher in system, must not have right to authorize payments.

- Maker must not be checker.

Auditor needs to check that there is no violation of above principle. Any violation may have serious repercussions, the same needs to be immediately communicated to those charged with governance.

Question 13

Discuss Managerial Controls and their Audit Trails.

Answer

The Managerial controls and their Audit trails are as follows:

(a) Top Management and Information Systems Management Controls: The major activities that senior management must perform are – Planning, Organizing, Controlling and Leading.

- *Planning: Auditors evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not.*
- *Organizing: Auditors should be concerned about how well top management acquires and manage staff resources.*
- *Leading: Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function.*
- *Controlling: Auditors must evaluate whether top management's choice to the means of control over the users of Information System services is likely to be effective or not.*

(b) System Development Management Controls: Three different types of audits may be conducted during system development process as follows:

- *Concurrent Audit: Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.*
- *Post -implementation Audit: Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.*
- *General Audit: Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.*

(c) Programming Management Controls: Some of the major concerns that an Auditor should address under different activities are as under:

- *Planning: They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired and how well the planning work is being undertaken.*
- *Control: They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. They must gather evidence on whether the control procedures are operating reliably.*
- *Design: Auditors should find out whether programmers use some type of systematic approach to design. Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.*
- *Coding: Auditors should seek evidence on the level of care exercised by programming management in choosing a module implementation and integration strategy. Auditors determine whether programming management ensures that programmers follow structured programming conventions.*
- *Testing: Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. They are concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users.*
- *Operation and Maintenance: Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs*

(d) Data Resource Management Controls: Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls. Auditors might employ test data to evaluate whether access controls and update controls are working.

(e) Quality Assurance Management Controls: Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role. Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.

(f) Security Management Controls: Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and check whether the organizations have opted for an appropriate insurance plan or not.

(g) <u>Operations Management Controls</u>: Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel. Auditors can use interviews, observations, and review of documentation to evaluate the activities of documentation librarians; how well operations management undertakes the capacity planning and performance monitoring function; the reliability of outsourcing vendor controls; whether operations management is monitoring compliance with the outsourcing contract; and Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

Question 14

As an IS auditor, what are the risks reviewed by you relating to IT systems and processes as part of your functions?

Answer

IS (Information Systems) Auditors review risks relating to IT systems and processes; some of them are as follows:

- *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.).*
- *IT-related frauds (including phishing, hacking etc).*

Question 15

Compared to traditional audit, evidence collection has become more challenging with the use of computers to the auditors. What are the issues which affect evidence collection and understanding the reliability of controls in financial audit?

Answer

The issues which affect evidence collection and understanding the reliability of controls in financial audit are as follows:

- *<u>Data retention and storage:</u> A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system.*

- ***Absence of input documents:*** *Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.*
- ***Non-availability of audit trail:*** *The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.*
- ***Lack of availability of output:*** *The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.*
- ***Audit evidence:*** *Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalized) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.*
- ***Legal issues:*** *The use of computers to carry out trading activities is also increasing. More organizations in both the public and private sector intend to make use of EDI and electronic trading over the internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and the parties to the contract.*

Question 16

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.

Answer

As a part of preliminary evaluation, the major aspects which should be studied to gain a good understanding of the technology environment and related control issues are as follows:

- *Analysis of business processes and level of automation,*

- *Assessing the extent of dependence of the enterprise on Information Technology 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 architecture or a centralized architecture 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 and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,*
- *And finally, studying Information Technology policies, standards, guidelines and procedures.*

Question 17

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.

Answer

Information Systems (IS) audit process can broadly be categorized on the basis of audit of Systems and applications; Information processing facilities; Systems Development; IT management and enterprise architecture; and Telecommunications, Intranets and Extranets.

Different auditors go about IS auditing in different ways. However, broadly the steps involved in an IS audit process are as follows:

(i) Scoping and pre-audit survey: Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management.

(ii) Planning and preparation: During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) Fieldwork: Gathering evidences by interviewing staff and managers; reviewing documents, and observing processes etc.

(iv) *__Analysis:__ This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.*

(v) *__Reporting:__ Reporting to the management is done after analysis of evidence gathered and analyzed.*

(vi) *__Closure:__ Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.*

Question 18

State four major tasks performed by an Operating System while allowing users and their applications to share and access common resources.

Answer

Operating System is the computer control program that allows users and their applications to share and access common computer resources, such as processor, main memory, database and printers. Some of the major tasks performed by an Operating system are as follows:

- *__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.*
- *__Maintaining 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 Resource 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.*
- *__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.*

Exercise

1. *What are the factors that influence an organization towards controls and audit of computers?*
2. *Discuss the points relating to 'Legal Considerations and Audit Standards' to be considered by an IS auditor as a part of his/her preliminary review.*
3. *Discuss Integrated Test Facility (ITF) technique of continuous audit in detail with the help of examples.*
4. *Describe major tasks performed by an Operating System in brief.*
5. *What are the major aspects that should be thoroughly examined by an IS Auditor during the audit of Environmental Controls? Explain in brief.*
6. *Discuss audit trails of the following with reference to Application Controls in brief.*

   (a) Input Controls

   (b) Output controls

   (c) Communication Controls

   (d) Database Controls

   (e) Boundary Controls

   (f) Processing Controls
7. *Discuss major audit issues of Tactical Layer with reference to Application Security Audit.*
8. *Write short notes on the following:*

   (i) Basic Plan with reference to IS Audit

   (ii) Continuous Auditing

   (iii) Continuous and Intermittent Simulation (CIS) technique

   (iv) Strategic Layer with reference to application security audit

7

Information Technology Regulatory Issues

Basic Concepts

1. Information Technology Act, 2000: In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the **Information Technology Act, 2000**. Cyber laws are contained in the IT Act, 2000.This Act aims to provide the legal infrastructure for e-commerce in India and has a major impact for e-businesses and the new economy in India. The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability. The Act was amended in 2008 by Information Technology (Amendment) Act, 2008.

The provisions of the Information Technology Act 2000 and the amendments of 2008 are simple to understand and most of these are self-explanatory. As an auditor, it is important to understand the key provisions of the IT Act as it impacts and provides the basis for other compliances. For example, when tax audit is being performed and the client accounts are maintained in a computer, it is important for the auditor to know specific provisions and the impact of the data being maintained in electronic form. Further, if audit is being done as per Companies Act, then specific aspects of internal controls and risk management are to be reviewed by auditor.

The Act provides various definitions of different technological terms. The sections, which are found to be relevant and useful for chartered accountants have been covered. For details, candidates are required to refer the Study Material.

2. Requirements of IRDA for System Controls & Audit: The Insurance Regulatory and Development Authority of India (IRDA) is the apex body overseeing the insurance business in India. It protects the interests of policyholders, regulates, promotes and ensures orderly growth of insurance industry in India. IRDA has mandated that all insurance companies shall have their systems and processes audited at least once in three years by a Chartered

Accountancy Firm.

3. **Requirements of RBI for System Controls & Audit:** The Reserve Bank of India (RBI) is India's central banking institution, which regulates banking activities in India. IS audits are gaining importance as key processes are automated or enabled by technology. RBI has been at the forefront of recognizing and promoting IS Audit internally and across all the stakeholders including financial institutions. RBI has been proactive in providing guidelines on key areas of IT implementation by using global best practices. It has constituted various expert committees who review existing and future technology and related risks and provides guidelines, which are issued to all stakeholders.

Primarily, RBI suggests that senior management and regulators need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the IT related risks are managed.

4. **Requirements of SEBI for System Controls & Audit:** The Securities and Exchange Board of India (SEBI) is the regulator for the securities market in India. SEBI has to be responsive to the needs of three groups, which constitute the market:

- The issuers of securities,
- The investors, and
- The market intermediaries.

Mandatory audit of systems and processes of Stock Exchanges brings transparency in the complex workings, proves integrity of the transactions and builds confidence among stakeholders.

5. **Cyber Forensic and Cyber Fraud Investigation:** Cyber forensics is one of the latest scientific techniques that has emerged due to the effect of increasing computer frauds. To understand the term better, an understanding of the independent words will be useful. Cyber, means on ‘The Net’ that is online. Forensics is a scientific method of investigation and analysis techniques 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. Considering ‘Cyber’ and ‘Investigation’ together will lead us to conclude that ‘Cyber Investigation’ is an investigation method gathering digital evidences to be produced in court of law.

Increasing frauds across the cyber space, the sheer size, speed and value of the frauds has surprised law keepers. Fraudsters are always on the look-out to misuse any loop hole or weaknesses in the computer systems.

6. **National Cyber Security Policy 2013:** Considering the importance of information security, Government of India recently published the National Cyber Security Policy 2013 with the vision “*To build a secure and resilient cyberspace for citizens, business and Government*” and the mission “*To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities*

and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and cooperation".

Based on the key aspects of National Cyber Security Policy 2013, we can understand that Chartered Accountants in their role as accountants and auditors have another important role to play in ensuring compliance of security and also pro-actively provide assurance on the state of IT security in an enterprise.

7. ISO 27001: ISO/IEC 27001 (International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC)) defines how to organize information security in any kind of organization, profit or non-profit, private or state-owned, small or large.

ISO/IEC 27001:2005, part of the growing ISO/IEC 27000 family of standards, was an Information Security Management System (ISMS) standard published in October 2005 by ISO/IEC. Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information Security Management Systems – Requirements. It was superseded, in 2013, by ISO/IEC 27001:2013.

An ISMS is a systematic approach to managing confidential or sensitive information so that it remains secure (which means available, confidential and with its integrity intact). It encompasses people, processes and IT systems.

Four phases of ISMS: ISO 27001: 2005 prescribes 'how to manage information security through a system of information security management'. Such a management system, just like ISO 9001 or ISO 14001, consists of four phases that should be continuously implemented in order to minimize risks to the CIA of information.

These phases are given 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.

ISO/IEC 27001:2013 is the first revision of ISO/IEC 27001 that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System within the context of the organization. It is an information security standard that was published on 25th September 2013. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature. ISO 27001:2013 does not put so much emphasis on this cycle.

Structure

In the new structure, the Processing Approach, used in ISO27001:2005, and which houses the PDCA model, was eliminated. The reason for this is that the requirement is for continual improvement and PDCA is just one approach to meeting that requirement. There are other approaches, and organizations are now free to use them if they wish. The introduction also draws attention to the order in which requirements are presented, stating that the order does not reflect their importance or imply the order in which they are to be implemented.

ISO27001:2013 has ten short clauses, plus a long Annex, which covers the following:

Clause 1: Scope
Clause 2: Normative references
Clause 3: Terms and Definitions
Clause 4: Context of the organization
Clause 5: Leadership
Clause 6: Planning
Clause 7: Support
Clause 8: Operation
Clause 9: Performance evaluation
Clause 10: Improvement
Annex A: List of controls an their objectives

8. **Standard on Auditing 402:** Audit Considerations Relating to an Entity using Service Organization, SA 402 is a revised version of the erstwhile Auditing and Assurance Standard (AAS) 24, "Audit Considerations Relating to Entities Using Service Organizations" issued by the ICAI in 2002. The revised Standard deals with the user auditor's responsibility to obtain sufficient appropriate audit evidence when a user entity uses the services of one or more service organizations. SA 402 also deals with the aspects like obtaining an understanding of the services provided by a service organization, including internal control, responding to the assessed risks of material misstatement, Type 1 and Type 2 reports, fraud, non-compliance with laws and regulations and uncorrected misstatements in relation to activities at the service organization and reporting by the user auditor.

9. **ITIL (IT Infrastructure Library):** ITIL is a set of practices for IT Service Management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITILv3 and ITIL 2011 edition), ITIL is published in a series of five core publications, each of which covers an ITSM lifecycle stage. ITIL describes procedures, tasks and checklists that are not organization-specific and are used by an organization for establishing a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure competence. It is used to demonstrate compliance and to measure improvement.

This release of ITIL brought with it an important change of emphasis, from an operationally focused set of processes to a mature service management set of practice guidance. It also brought a rationalization in the number of volumes included in the set, which now comprises the following:

- **Service Strategy:** Service Strategy deals with the strategic management approach in respect of IT Service Management; strategic analysis, planning, positioning, and implementation relating to service models, strategies, and strategic objectives. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers.
- **Service Design:** Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations. It provides guidance on combining infrastructure, applications, systems, and processes, along with suppliers and partners, to present feasible service offerings.
- **Service Transition:** Service Transition provides guidance on the service design and implementation, ensuring that the service delivers the intended strategy and that it can be operated and maintained effectively.
- **Service Operation:** Service Operation provides guidance on the management of a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.
- **Continual Service Improvement:** Continual Service Improvement provides guidance on the measurement of service performance through the service life-cycle, suggesting improvements to ensure that a service delivers the maximum benefit.

Question 1

Explain the objectives of the Information Technology Act 2000.

Answer

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.

Question 2

Define the following terms with reference to Information Technology Act 2000:

(i) Digital signature

(ii) Electronic form

(iii) Key Pair

(iv) Asymmetric Crypto System

Answer

(i) Digital Signature: It means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

(ii) Electronic form: With reference to information, it means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.

(iii) Key Pair: In an asymmetric cryptosystem, it means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

(iv) Asymmetric Crypto System: It is 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.

Question 3

Explain 'Authentication of Electronic Records' with reference to Section 3 of Information Technology Act 2000.

Or

How does the Information Technology Act 2000 enable the authentication of records using digital signatures?

Answer

***[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.

Question 4

Discuss the main provisions provided in Information Technology Act 2000 to facilitate e-Governance.

Answer

e-Governance sections of chapter III 6, 7 and 8 are the main sections for provisions related to e-Governance provided in Information Technology Act 2000 to facilitate e-governance.

Section 6 lays down the foundation of electronic Governance. It provides that the filling of any form, application or other documents; creation, retention or preservation of records, issue or grant of any license or permit; receipt or payment in Government offices and its agencies may be done by means of electronic form. The appropriate Government has the power to prescribe the manner and format of the electronic records.

Section 7 provides legal sanctity and documents, records or information can be retained in electronic form thus removing the need to retain it in physical form. To safeguard the information even when technology changes, it provides that:

(i) It should be possible to access and use the information later;

(ii) Whenever the original format of the information is changed (e.g. due to technology) the new content should accurately represent the original information; and

(iii) The document should contain details to identify the origin, destinations, dates and time of dispatch or receipt of such electronic record (e.g. when emails or logs are stored).

Section 8 provides that rules, regulations, orders, bye-laws and notifications required under any law to be published in the official Gazette can be published in the electronic gazette substituting the need for manual documents.

Question 5

Discuss the 'Use of Electronic Records in Government and its agencies' in the light of Section 6 of Information Technology Act 2000.

Answer

Section 6 provides for use of electronic records in government and its agencies even though the original law requiring these documents did not provide for electronic forms. It allows use of electronic form for:

- filing any form, application or other documents;
- creation, retention or preservation of records, issue or grant of any license or permit;
- receipt or payment of money in Government offices.

The appropriate Government has the power to prescribe the manner and format of the electronic records

Question 6

Describe the 'Power to make rules by Central Government in respect of Electronic Signature' in the light of Section 10 of Information Technology Act 2000.

Answer

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 the manner and format in which the Electronic Signature shall be affixed;

(c) specify the manner or procedure which facilitates identification of the person affixing the Electronic Signature;

(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to Electronic Signature.

Question 7

Describe the 'Tampering with Computer Source Documents' in the light of Section 65 of Information Technology Act 2000.

Answer

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programme, computer commands, design and layout and program analysis of computer resource in any form.

Question 8

Discuss 'Power of the Controller to give directions' under Section 68 of Information Technology Act 2000.

Answer

Certifying Authorities create digital signatures and provide them to subscribers. People use and rely on Digital signatures for carrying on electronic commerce. If signatures are compromised, or if there are insufficient safeguards over their creation or provision, the system will be weakened. To prevent this, the Controller is provided following powers:

[Section 68] **Power of Controller to give directions**

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or with both.

Question 9

Discuss 'Power to issue directions for interception or monitoring or decryption of any information in any computer resource' under Section 69 of Information Technology Act 2000.

Answer

Section 69 gives powers to Central & State Governments to issue directions empowering a Government agency to intercept, monitor or decrypt any information through or in any computer if it is for important purposes as specified in the section. These include:

(1) Where the Central Government or a State Government or any of its officers specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

(2) The Procedure and safeguards over such interception or monitoring or decryption, shall be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by the agency, extend all facilities and technical assistance to -

 (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

 (b) intercept, monitor, or decrypt the information, as the case may be; or

 (c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist such agency shall be punished with imprisonment up to seven years and fine.

Question 10

Discuss 'Penalty for publishing Electronic Signature Certificate false in certain particulars' under Section 73 of Information Technology Act 2000.

Answer

[Section 73] Penalty for publishing Electronic Signature Certificate false in certain particulars

(1) No person shall publish a Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that -

 (a) the Certifying Authority listed in the certificate has not issued it; or

 (b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Question 12

What is the vision of National Cyber Security Policy 2013? Also explain its major objectives.

Answer

Vision of the National Cyber Security Policy 2013 is: "*To build a secure and resilient cyberspace for citizens, business and Government*" and the mission "*To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people processes, technology and cooperation*".

Major objectives of this policy are given as follows:

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy;
- To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology, & people);
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem;
- To enhance and create National and Sectorial level 24*7 mechanisms for obtaining strategic information regarding threats of ICT infrastructure creating scenarios for response, resolution and crisis management through effective predicative, protective, response and recovery actions;
- To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24*7 National Critical Information Infrastructure Protection Center(NCIIPC) and mandating security practices related to the design, acquisition, development and operation of information resources;
- To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, and pilot development of secure ICT products/processes in general and specifically for addressing National Security requirements;

- To improve visibility of the integrity of ICT products & services and establishing infrastructure for testing & validation of security of such products;
- To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training;
- To provide fiscal benefits to businesses for adoption of standard security practices and processes;
- To enable protection of information while in process, handling, storage & transit so as to Safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft;
- To enable effective prevention, investigation and prosecution of cybercrime and enhancements of law enforcement capabilities through appropriate legislative intervention;
- To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy;
- To develop effective public private partnerships and collaborative engagements through technical and operational collaboration and contribution for enhancing the security of cyberspace and
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Question 12

Discuss PDCA cyclic process under ISO27001.

Answer

The Plan-Do-Check-Act (PDCA) cycle

ISO27001 prescribes 'How to manage information security through a system of information security management'. Such a management system consists of four phases that should be continuously implemented in order to minimize risks to the Confidentiality, Integrity and Availability (CIA) of information.

The PDCA cyclic process is explained below:

- **The Plan Phase (Establishing the ISMS) –** 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 (Implementing and Working of ISMS) –** This phase includes carrying out everything that was planned during the previous phase.

- **The Check Phase (Monitoring and Review of the ISMS) –** 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 (Update and Improvement of the ISMS) –** 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. ISO/IEC 27001:2005 applies this to all the processes in ISMS.

Question 13

Write a short note on ‘Service Strategy’ of IT Infrastructure Library (ITIL) framework.

Answer

Service Strategy: The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service-provider investments in services. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers. The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset. It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

- **IT Service Generation:** IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.
- **Service Portfolio Management:** IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.
- **Financial Management:** Financial Management for IT Services’ aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.
- **Demand Management:** Demand management is a planning methodology used to manage and forecast the demand of products and services.
- **Business Relationship Management:** Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.

Question 14

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.

Answer

(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.

Question 15

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.

Answer

SEBI (Securities and Exchange Board of India) mandated that exchanges shall conduct an annual system audit by a reputed independent auditor.

- *The Audit shall be conducted according to the Norms, Terms of References (TOR) and Guidelines issued by SEBI.*
- *Stock Exchange/Depository (Auditee) may negotiate and the board of the Stock Exchange / Depository shall appoint the Auditors based on the prescribed Auditor Selection Norms and TOR. The Auditors can perform a maximum of 3 successive audits. The proposal from Auditor must be submitted to SEBI for records.*
- *Audit schedule shall be submitted to SEBI at-least 2 months in advance, along with scope of current audit & previous audit.*
- *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 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 reports in consideration and cover any open items therein.*
- *The Auditee management provides their comment about the Non-Conformities (NCs) 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 the status of NCs. The report along with Management Comments shall be submitted to SEBI within 1 month of completion of the audit.*

Question 16

Discuss briefly, the four phases of Information Security Management System (ISMS) prescribed by ISO 27001.

Answer

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.

Question 17

The manner of selecting auditors builds confidence among various stakeholders. Describe SEBI norms for selecting an auditor.

Answer

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)²^2.***
- ***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.***

Exercise

1. *What are the major provisions on 'Retention of Electronic Records' with reference to Information Technology Act 2000? Explain in brief.*
2. *Briefly explain the following with respect to the Information Technology Act 2000:*

   (i) [Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device

   (ii) [Section 66C] Punishment for identity theft

   (iii) [Section 66D] Punishment for cheating by personation by using computer resource

   (iv) [Section 66E] Punishment for violation of privacy

   (v) [Section 66F] Punishment for cyber terrorism

3. *Explain the 'Power to issue directions for blocking public access of any information through any computer resource' under Section 69A of the Information Technology Act 2000.*

4. *Explain the 'Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security' with reference to Section 69B of the Information Technology Act 2000.*

5. *Write short notes on the following:*

   (i) [Section 4] Legal Recognition of Electronic Records

   (ii) [Section 5] Legal Recognition of Electronic Signature

6. *Write short notes on the following:*

   (i) System Controls with reference to the requirement of RBI for System Control and Audit

   (ii) Auditor Selection Norms with reference to the requirement of SEBI for System Control and Audit

7. *Discuss ITIL framework.*

8

Emerging Technologies

Basic Concepts

1. Cloud Computing: Cloud computing simply means the use of computing resources as a service through networks, typically the Internet. Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service. This model of IT enabled services enables anytime access to a shared pool of applications and resources.

With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software. Cloud computing is of particular benefit to small and medium-sized business systems, who wish to completely outsource their data-center infrastructure; or large companies, who wish to get peak load capacity without incurring the higher cost of building larger data centers internally. In both the instances, service consumers use '*what they need on the Internet'* and *pay only for 'what they use'*.

2. Cloud v/s Grid Computing: Some pertinent similarities and differences are:

- Cloud Computing and Grid Computing both are scalable.
- Both computing types involve multi-tenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances.
- While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
- A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

3. Goals of Cloud Computing: The core goal of utilizing a cloud-based IT ecosystem is to pool available resources together into a highly efficient infrastructure whose costs are aligned with what resources are actually used to make the services accessible and available from anywhere at any time.

4. Cloud Computing Architecture: The Cloud Computing Architecture (CCA) of a cloud solution is the structure of the system, which comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them. Cloud architecture typically involves multiple cloud components communicating with each other over a loose coupling mechanism, such as a messaging queue. This is depicted in Fig. 8.1, which is given as follows:

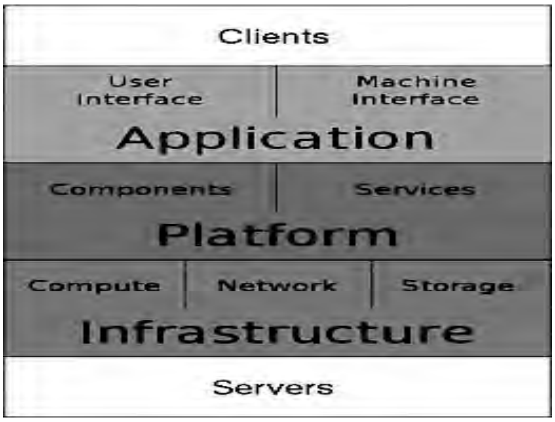


Fig. 8.1: Cloud Computing Architecture

5. Cloud Computing Environment/Deployment Models: The cloud computing environment can consist of multiple types of clouds based on their deployment and usage. These are:

(a) **Public Clouds:** This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called provider clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.

(b) **Private Clouds:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization. ***Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud).***

(c) **Hybrid Clouds:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

(d) ***Community Clouds:*** ***The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations.***

6. **Cloud Computing Service Models:** These are as follows:

(a) **Infrastructure as a Service (IaaS):** IaaS providers offer computers, more often virtual machines and other resources as service. It provides the infrastructure / storage required to host the services ourselves i.e. makes us the system administrator and manage hardware/storage, network and computing resources. The different instances of IaaS are as follows:

- **Network as a Service (NaaS):** It is a category of cloud services where the capability provided to the cloud service user is to use network/transport connecting services. NaaS involves optimization of resource allocation by considering network and computing resources as a whole.

    - ***Storage as a Service (STaaS):*** ***STaaS, an instance of IaaS, provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devises, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term.***

    - ***Database as a Service (DBaaS):*** ***This is also related to IaaS and provides users with seamless mechanisms to create, store, and access databases at a host site on demand.***

    - ***Backend as a Service (BaaS):*** ***It is a type of IaaS, that provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.***

    - ***Desktop as a Service (DTaaS):*** ***It is an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure.***

- **Platform as a Service** (**PaaS**): ***PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider.*** Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server. ***For example- Google AppEngine, Windows Azure Compute etc.***

(c) Software as a Service (SaaS): SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. ***Thus, the end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure. SaaS changes the way the software is delivered to the customers.***

- ***Testing as a Service (TaaS): This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.***
- ***API as a Service (APIaaS): This allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.***
- ***Email as a Service (EaaS): This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.***

(e) Other Cloud Service Models:

- **Communication as a Service (CaaS):** CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vendor. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates large capital investments.
- ***Data as a Service (DaaS): DaaS provides data on demand to a diverse set of users, systems or application. The data may include text, images, sounds, and videos. Data encryption and operating system authentication are commonly provided for security.***
- ***Security as a Service (SECaaS): It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats.***
- ***Identity as a Service (IDaaS): It is an ability given to the end users; typically an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed and provided by the third party service provider.***

7. Characteristics of Cloud Computing: Major characteristics are: High Scalability, Agility, High Availability and Reliability, Multi-sharing, Services in Pay-Per-Use Mode, Virtualization, Performance, and Maintenance.

8. **Advantages of Cloud Computing:** Major advantages of Cloud Computing are: Cost Efficiency, Almost Unlimited Storage, Backup and Recovery, Automatic Software Integration, Easy Access to Information, and Quick Deployment.

9. **Challenges to Cloud Computing**: Major challenges are: Confidentiality, Integrity, Availability, Governance, Trust, Legal Issues and Compliance, Privacy, Audit, Data-Stealing, Architecture, Identity Management and Access control, Incident Response, Software Isolation and Application Security.

10. **Mobile Computing:** It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution for the biggest problem of business people on the move i.e. mobility.

Various companies design and develop several wireless applications and solutions for Blackberry, iPhone, Google Android G1, iPad, Windows Mobile, Symbian, Brew devices, PDA, Palm & Pocket PC. Mobile Computing Services allow mobile workforces to access a full range of corporate services and information from anywhere, at any time and it improves the productivity of a mobile workforce by connecting them to corporate information systems and by automating paper-based processes.

11. **BYOD:** 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.

12. **Emerging BYOD Threats:** Overall, these can be classified into four areas as outlined below:

- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network.
- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information.
- **Application Risks:** It is normally exemplified and hidden in **'**Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software.

- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy.

13. Social Media: A social network is usually created by a group of individuals, who have a set of common interests and objectives. There are usually a set of network formulators followed by a broadcast to achieve the network membership. This happens both in public and private groups depending upon the confidentiality of the network.

14. Web 2.0: Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users.

Components of Web 2.0 for Social Networks: Major components that have been considered in Web 2.0 include the following: Communities, ***RSS-generated Syndication*****,** Blogging, Wikis, ***Usage of Ajax and other new technologies,*** Folksonomy, File Sharing/Podcasting, and Mash-ups.

15. Web 3.0: Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users. Web 3.0 technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence.

An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence.

16. 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.

It is largely taken as the study and practice of designing, manufacturing, using, and disposing of computers, servers, associated subsystems and peripheral devices efficiently and effectively with highly mitigated negative impact on the environment. The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.

Question 1

What is Cloud Computing? Explain some pertinent similarities and differences between Cloud and Grid computing.

Answer

Cloud Computing: Cloud computing simply means the use of computing resources as a service through networks, typically the Internet. With Cloud Computing, users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. The best example of cloud computing is *Google Apps* where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.

Cloud computing is both, a combination of software and hardware based computing resources delivered as a networked service. With cloud computing, companies can scale up to massive capacities in an instant without having to invest in new infrastructure, train new personnel or license new software.

Some pertinent similarities and differences between cloud and grid computing are highlighted as follows:

- Cloud computing and grid computing both are scalable. Scalability is accomplished through load balancing of application instances running separately on a variety of operating systems and connected through Web services. CPU and network bandwidth is allocated and de-allocated on demand. The system's storage capacity goes up and down depending on the number of users, instances, and the amount of data transferred at a given time.
- Both computing types involve multi-tenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances. Sharing resources among a large pool of users assists in reducing infrastructure costs and peak load capacity. Cloud and grid computing provide Service-Level Agreements (SLAs) for guaranteed uptime availability of, say, 99 percent. If the service slides below the level of the guaranteed uptime service, the consumer will get service credit for not receiving data within stipulated time.
- While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.
- A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

Question 2

Discuss the major goals of Cloud Computing in brief.

Answer

Major goals of cloud computing are as follows:

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

Question 3

Describe Front End and Back End architecture with reference to Cloud Computing.

Answer

Front End Architecture: The front end of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.

Back End Architecture: Back end refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.

Question 4

What do you understand by Public cloud? Also discuss its major advantages and limitations in brief.

Answer

Public Clouds: This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called provider clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.

The Advantages of public cloud include the following:

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- ***There is no need for establishing infrastructure for setting up and maintaining the cloud.***
- ***Strict SLAs are followed.***
- ***There is no limit for the number of users.***

  Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen. ***Further, privacy and organizational autonomy are not possible.***

Question 5

What is Private cloud? Also explain its major advantages and limitations in brief.

Answer

Private Clouds: This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

The advantages of private clouds include the following:

- They improve average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies; thus reducing the costs that a greater number of servers would otherwise entail.
- ***It provides a high level of security and privacy to the user.***
- ***It is small in size and controlled and maintained by the organization.***

Moreover, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently***. Budget is a constraint in private clouds and they also have loose SLAs.***

However, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently.

Question 6

Explain the characteristics of the following with reference to cloud computing:

(i) Infrastructure as a Service (IaaS)

(ii) Platform as a Service (PaaS)

(iii) Software as a Service (SaaS)

Answer

(i) ***Characteristics of Infrastructure as a Service (IaaS) are as follows:***

- ***Web access to the resources: The IaaS model enables the IT users to access infrastructure resources over the /Internet. When accessing a huge computing power, the IT user need not get physical access to the servers.***
- ***Centralized management: The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.***
- ***Elasticity and Dynamic Scaling: Depending on the load, IaaS services can provide the resources and elastic services where the usage of resources can be increased or decreased according to the requirements.***
- ***Shared infrastructure: IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensure high resource utilization.***
- ***Metered Services: IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.***

(ii) ***Characteristics of Platform as a Service (PaaS) are as follows:***

- ***All in One: Most of the PaaS providers offer services like programming languages to develop, databases, test, deploy, host and maintain applications in the same Integrated Development Environment (IDE).***
- ***Web access to the development platform: PaaS provides web access to the development platform that helps the developers to create, modify, test, and deploy different applications on the same platform.***
- ***Offline Access: To enable offline development, some of the PaaS providers allow the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.***

- ***Built-in Scalability:*** ***PaaS services provide built-in scalability to an application that is developed using any particular PaaS. This ensures that the application is capable of handling varying loads efficiently.***
- ***Collaborative Platform:*** ***To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.***
- ***Diverse Client Tools:*** ***PaaS providers offer a wide variety of client tools like Web UI, API etc. to help the developers to choose the tool of their choice.***

(iii) *Characteristics of Software as a Service (SaaS) are as follows:*

- ***One to Many:*** ***SaaS services are delivered as one-to-many models where a single instance of the application can be shared by multiple customers.***
- ***Web Access:*** ***SaaS services allow the end users to access the application from any location of the device is connected to the Internet.***
- ***Centralized Management:*** ***Since SaaS services are hosted and managed from the central location, the SaaS providers perform the automatic updates to ensure that each customer is accessing the most recent version of the application without any user-side updates.***
- ***Multi-device Support:*** ***SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smartphones, and thin clients.***
- ***Better Scalability:*** ***Most of the SaaS services leverage PaaS and IaaS for its development and deployment and ensure a better scalability than traditional; software.***
- ***High Availability:*** ***SaaS services ensure 99.99% availability of user data as proper backup and recovery mechanisms are implemented.***
- ***API Integration:*** ***SaaS services have the capability of integrating with other software or service through standard APIs.***

Question 7

Explain, in brief, the characteristics of Cloud Computing.

Answer

Major characteristics of cloud computing are given as follows:

- **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 Mode:** SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.
- **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- **Performance:** It is monitored and consistent and its loosely coupled architecture constructed using web services as the system interface enables high level of performance.
- **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.

Question 8

Briefly discuss the advantages of Cloud Computing.

Answer

Major advantages of Cloud Computing are given as follows:

- **Cost Efficiency:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot in terms of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned. The cloud, on the other hand, 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. Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.
- **Backup and 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. Furthermore, most cloud service providers are usually competent enough to handle

recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

- **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. This aspect usually takes care of itself. Not only that, cloud computing allows us to customize the options with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her particular enterprise.
- **Easy Access to Information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.
- **Quick Deployment:** 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. Of course, the amount of time taken here will depend on the exact kind of technology that we need for our business.

Question 9

Discuss any four challenges to Cloud computing in brief.

Answer

Four challenges to cloud computing are given as follows:

- **Confidentiality:** Prevention of unauthorized disclosure of data is referred to as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control).
- **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be ensured that the data is not changed after being moved to the cloud. It is important to verify if one’s data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.

- **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete. Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability. One of the major Cloud service provider, AWS had a breakdown for several hours, which led to data loss and access issues with multiple Web 2.0 services.
- **Architecture:** In the architecture of Cloud computing models, there should be control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework.

Question 10

Explain some of the tangible benefits of mobile computing.

Answer

Major tangible benefits of mobile computing are given as follows:

- 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 us to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

Question 11

Write short notes on the following:

(i) Hybrid Cloud

(ii) Mobile Computing

(iii) BYOD

(iv) Web 2.0

(v) Green IT

Answer

(i) **Hybrid Cloud:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms.

(ii) **Mobile Computing:** It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution of the biggest problem of business people on the move i.e. mobility.

(iii) **BYOD:** 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. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, challenging the long-standing policy of working on company-owned devices. Though it has led to an increase in employees' satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

(iv) **Web 2.0:** Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability of people to collaborate and share information online. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information. Over the time, Web 2.0 has been used more as a marketing term than a Computer Science based term. Blogs, wikis, and Web services are all seen as components of Web 2.0. Web 2.0 tries to tap the power of humans connected electronically through its new ways at looking at social collaboration. The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner. In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mash-ups, and Tagging. The power of Web 2.0 is the creation of new relationships between collaborators and information.

(v) **Green IT**: Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient, environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle. It is largely taken as the study and practice of designing, manufacturing, using, and disposing of computers, servers, associated subsystems and peripheral devices efficiently and effectively with highly mitigated negative impact on the environment. The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.

Question 12

'The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment'. Discuss some of such steps, which can be followed for Green IT.

Or

Discuss best practices of Green IT.

Answer

Some of such steps for Green IT include the following:

<u>Develop a sustainable Green computing plan</u>

- ***Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;***
- Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
- On-going communication about and campus commitment to green IT best practices to produce notable results.

- ***Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans; and***
- ***Use cloud computing so that multiple organizations share the same computing resources thus increasing the utilization by making more efficient use of hardware resources.***

Recycle

- ***Dispose e-waste according to central, state and local regulations;***
- ***Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;***
- ***Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and***
- ***Recycle computers through manufacturer's recycling services.***

Make environmentally sound purchase decisions

- ***Purchase of desktop computers, notebooks and monitors based on environmental attributes;***
- ***Provide a clear, consistent set of performance criteria for the design of products;***
- ***Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and***
- ***Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.***

Reduce Paper Consumption

- ***Reduce paper consumption by use of e-mail and electronic archiving;***
- ***Use of "track changes" feature in electronic documents, rather than redline corrections on paper;***
- ***Use online marketing rather than paper based marketing; e-mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste; and***
- ***While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.***

Conserve Energy

- *Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;*
- *Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;*
- *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;*
- *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;*
- *Employ alternative energy sources for computing workstations, servers, networks and data centers; and*
- *Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.*

Question 13

Discuss some of the pertinent objectives in order to achieve the goals of Cloud Computing.

Answer

Some of the pertinent objectives in order to achieve the goals of Cloud Computing are as follows:

- *To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;*
- *To access services and data from anywhere at any time;*
- *To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;*
- *To consolidate IT infrastructure into a more integrated and manageable environment;*
- *To reduce costs related to IT energy/power consumption;*

- *To enable or improve "Anywhere Access" (AA) for ever increasing users; and*
- *To enable rapidly provision resources as needed.*

Question 14

Discuss the Security and Implementation issues in using Cloud Computing technology for running the new web application.

Answer

Major challenges in Cloud Computing Technology for running new Web application are as follows:

(A) **Security Issues:** Security is a major issue relating to cloud computing. Some of the major security issues are discussed below:

- ***Confidentiality: Prevention of the unauthorized disclosure of the data is referred as Confidentiality. With the use of encryption and physical isolation, data can be kept secret.***
- ***Integrity: Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible.***
- ***Availability: Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure and natural calamities are all threats to availability.***
- ***Governance: Due to the lack of control over the employees and services, there is problem relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization.***
- ***Trust: Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.***
- ***Legal Issues and Compliance: There are various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements.***
- ***Privacy: The privacy issues are embedded in each phase of the Cloud design that includes both the legal compliance and trusting maturity.***

- *<u>Audit:</u> Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'.*

- *<u>Data Stealing:</u> In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. Some of the Cloud providers use server/s from other service providers and thus there is a probability that the data is less secure and is more prone to the loss from external server.*

- *<u>Architecture:</u> In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The reliability and scalability of architecture is dependent on the design and implementation to support the overall framework.*

- *<u>Identity Management and Access control:</u> A robust federated identity management architecture and strategy internal in the organization provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.*

- *<u>Incident Response:</u> It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.*

- *<u>Software Isolation:</u> Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture and evaluate the risks required for the organization.*

- *<u>Application Security:</u> Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server.*

(B) <u>Implementation/Adaptation Issues:</u> Some of the well-identified implementation issues are as follows:

- *<u>Threshold Policy:</u> This involves the checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de-allocated and turned over to other work needs to work out in the context.*

- *<u>Interoperability:</u> If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another*

computing vendor that has proprietary Application Programming Interfaces (APIs) and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors.

- ***<u>Hidden Costs:</u> Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another instance of incurring network costs, companies, who are far from the location of cloud providers, could experience latency, particularly when there is heavy traffic.***
- ***<u>Unexpected Behavior:</u> Let's suppose that credit card validation application works well at our company's internal data centre. It is important to test the application in the cloud with a pilot study to check for unexpected behavior. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud.***

  Instead of waiting for an outage to occur, consumers should do security testing on their own checking how well a vendor can recover data. Apart from the common testing practices, what one needs primarily to do is to ask for old stored data and check how long it takes for the vendor to recover. If it takes too long to recover, ask the vendor why and how much service credit we would get in different scenarios. Moreover, in such cases, verifying the checksums match with the original data is a requisite.

  Another area of security testing is to test a trusted algorithm to encrypt the data on the local computer, and then try to access data on a remote server in the cloud using the decryption keys. If we can't read the data once we have accessed it, the decryption keys are corrupted, or the vendor is using its own encryption algorithm. We may need to address the algorithm with the vendor. Another issue is the potential for problems with data in the cloud. To protect the data, one may want to manage his/her own private keys. Checking with the vendor on the private key management is no longer a simple as it appears so.
- ***<u>Software Development in Cloud:</u> To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project***

managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud. The cost associated with each cloud type may differ from one another. The cost per hour or usage with the development cloud is most likely lower than the production cloud, as additional features, such as SLA and security, are allocated to the production cloud. The managers can limit projects to certain clouds. For instance, services from portions of the production cloud can be used for the production configuration. Services from the development cloud can be used for development purpose only. To optimize assets at varying stages of the project of software development, the managers can get cost-accounting data by tracking usage by project and user.

- *Environment Friendly Cloud Computing: One incentive for cloud computing is that it may be more environment friendly. First, reducing the number of hardware components needed to run applications on the company's internal data centre and replacing them with cloud computing systems reduces energy for running and cooling hardware. By consolidating these systems in remote centers, they can be handled more efficiently as a group.*

Question 15

List major advantages and limitations of Hybrid Cloud, in brief.

Answer

The Advantages of Hybrid Cloud include the following:

- *It is highly scalable and gives the power of both private and public clouds.*
- *It provides better security than the public cloud.*

The limitation of Hybrid Cloud is that the security features are not as good as the public cloud and complex to manage.

Question 16

What is Community Cloud? Discuss its advantages and limitations in brief.

Answer

Community Cloud: The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may *exist on or off premises. In this, a private cloud is shared between several organizations.*

Advantages of Community Clouds are as follows:

- *It allows establishing a low-cost private cloud.*
- *It allows collaborative work on the cloud.*
- *It allows sharing of responsibilities among the organizations.*
- *It has better security than the public cloud.*

The limitation of the community cloud is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the cases where there is no collaboration.

Question 17

Discuss the components of Mobile Computing.

Answer

The key components of Mobile Computing are as follows:

- *Mobile Communication: This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.*
- *Mobile Hardware: This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network (this server provide communications functionality to allow the handheld device to communicate with the internet or Intranet Infrastructure). The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.*
- *Mobile Software: Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks, in terms of flow of data as well as personal*

identification risks, introduction of malware and access to personal information of mobile owner.

Question 18

Discuss security issues of Mobile Computing.

Answer

- ***<u>Security Issues</u>: Wireless networks have relatively more security requirements than wired network. A number of approaches have been suggested and also the use of encryption is has been proposed.***
  - ***<u>Confidentiality</u>: Preventing unauthorized users from gaining access to critical information of any particular user.***
  - ***<u>Integrity</u>: Ensures unauthorized modification, destruction or creation of information cannot take place.***
  - ***<u>Availability</u>: Ensuring authorized users getting the access they require.***
  - ***<u>Legitimate</u>: Ensuring that only authorized users have access to services.***
  - ***<u>Accountability</u>: Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked if and when necessary.***

Exercise

1. *Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are two of the three main categories of cloud computing. What's the third category? Explain in brief.*
2. *Explain components of Web 2.0 for Social Networks.*
3. *Discuss limitations of Mobile Computing.*
4. *Discuss pertinent issues of Mobile Computing.*
5. *Discuss advantages of Bring your own Device (BYOD).*

Questions Based on the Case Studies

Question 1

PQR University is a public university; especially known for its Faculty of Commerce and Management in the country. The faculty offers various UG and PG programs along with research studies viz. M. Phil and Ph.D. Recently, the Academic Council of the university approved the proposal of the faculty to start some UG and PG courses in distance learning mode too. It is observed that the students of distance education are normally dependent on self-study only along with a little support from the concerned department/s. In view of this aforementioned fact, the concerned Dean of the faculty decided to launch a web based Knowledge Portal to facilitate the students of different courses. It is proposed to upload the Study Materials, e-lectures, Suggested Answers of last examinations, Mock Test Papers relevant for the coming examinations etc. of the approved courses on this Knowledge Portal. It is expected that the portal will be very useful for the students as it aims to provide the access of various academic resources on anytime anywhere basis. For the implementation of this project, a technical consultant was appointed by the university. Accordingly, an initial feasibility study under various dimensions was done and a detailed report was submitted. As a next step, as per the recommendations of the consultant, an expression of interest was published by the University in various national/regional newspapers inviting various organizations to showcase their capabilities and suggest a good solution as per the requirements of the concerned faculty of the university.

Read the above carefully and answer the following:

(a) What are three major attributes of information security? Out of these attributes, which attribute will be having the highest priority while developing web based knowledge portal?

(b) What may be the possible dimensions under which the feasibility study of the proposed Knowledge Portal was done in your opinion?

(c) What may be the major validation methods for validating the vendors' proposal for developing the Knowledge Portal?

Answer

(a) Three major attributes of information security are given as follows:

- **Confidentiality:** It refers to the prevention of unauthorized disclosure of information.
- **Integrity:** It refers to the prevention of unauthorized modification of information.
- **Availability:** It refers to the prevention of unauthorized withholding of information.

The proposed Knowledge Portal aims to provide the access of various academic resources on anytime anywhere basis. Hence, out of these aforementioned attributes, the third attribute namely, availability will be having the highest priority while developing web based knowledge portal.

(b) The possible dimensions under which the feasibility study of the proposed Knowledge Portal was done are given as follows:

- **Technical:** Is the technology needed to build and run the portal available?
- **Financial:** Is the solution financially viable? (e.g. revenue from new course vis-à-vis reduction in cost of classrooms / new cost of developing and running portal)
- **Economic:** What is the Return on Investment?
- **Schedule/Time:** Can the system be delivered on time? (e.g. before start of the new academic year)
- **Resources:** Are human resources (faculty) available to develop the solution or are they reluctant to use it?
- **Operational:** How will the solution work?
- **Behavioral:** Is the solution going to bring any adverse or positive effect on quality of work life? (e.g. enable students to pursue studies at their own time and from their own place of stay without having to be on campus; effect on students / their study due to non-interaction with other students and faculty)
- **Legal:** Is the solution valid in legal terms? E.g. considering the requirements specified by University regulators like UGC – University Grants Commission

(c) Major validation methods of validating the vendors' proposal for developing the Knowledge Portal are given as follows:

- **Checklists:** It is the most simple and rather subjective method for validation and evaluation. The various criteria are put into check lists in the form of suitable questions against which the responses of the various vendors are validated. For example : Support Service Checklists may have parameters like – Performance, System development, Maintenance, Conversion, Training, Back-up, Proximity, Hardware, Software.
- **Point-Scoring Analysis:** Point-scoring analysis provides an objective means of selecting the final system. There are no absolute rules in the selection process, only guidelines for matching user needs with software capabilities. Evaluators must consider such issues as the University's needs to operate and maintain the portal, vendor reputations, software costs, user-friendliness for students (who are the customers in this case), and so forth.
- **Public Evaluation Reports**: Several consultancy agencies compare and contrast the hardware and software performance for various manufacturers and publish their reports in this regard. This method has been frequently and usefully employed by

several buyers in the past. For those criteria where published reports are not available, however, resort would have to be made to other methods of validation. This method is particularly useful where the buying staff has inadequate knowledge of facts. E.g. Public reports by agencies like Gartner's magic quadrant on systems used by other universities offering online courses may be considered

- **Benchmarking Problem for Vendor's Proposals:** Benchmarking problems for vendors' proposals are sample programs that represent at least a part of the buyer's primary computer work load and include software considerations and can be current applications programs or new programs that have been designed to represent planned processing needs. E.g. develop a set of sample requirements of a student and see whether the proposed system is able to effectively and efficiently deliver them. That is, benchmarking problems are oriented towards testing whether a computer system offered by the vendor meets the requirements of the buyer.
- **Test Problems:** Test problems disregard the actual job mix and are devised to test the true capabilities of the hardware, software or system. For example, test problems may be developed to evaluate the time required to download e-lectures (which are large sized files) by students, response time when large number of students login in at the same time, overhead requirements of the operating system in executing multiple user requests, length of time required to execute an instruction, etc. The results, achieved by the machine can be compared and price performance judgment can be made. It must be borne in mind, however that various capabilities to be tested would have to be assigned relative weightage as all requirements may not be equally important.

Question 2

ASK International proposes to launch a new subsidiary to provide e-consultancy services for organizations throughout the world, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programme modules and draft agreements are all preserved and administered in e-form only.

The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied. The company has been advised to adopt ISO 27001 for achieving the same.

(a) What are the two primary methods through which the analyst would have collected the data ?

(b) To retain their e-documents for specified period, what are the conditions laid down in Section 7, Chapter III of Information Technology Act, 2000?

Answer

(a) Two primary methods through which the analyst would have collected the data are given as follows:

(**i)** **Reviewing Internal Documents:** The analyst first tries to learn about the organization involved in or affected by the project. For example, the subsidiary's activities based on its business and operation plans. S/he will also examine proposed organization charts and functions of positions mentioned in it.

(ii) **Conducting Interviews:** Written documents tell the analyst 'how the system should operate' but they may not include enough details to allow a decision to be made about the merits of a system proposal nor do they present users' views about current operations. To learn these details, analysts use interviews. Preliminary investigation interviews involve only management and supervisory personnel. The analyst may conduct interviews with persons who are scheduled to occupy various positions in the subsidiary.

(b) Section 7, Chapter III of Information Technology Act, 2000 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

(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;

(c) 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.

E.g. Company may include clause in its contracts with customers that electronic documents and correspondence will be considered valid; Electronic documents will have to be preserved till the contract and all liabilities are discharged; Documents may be digitally signed with hash values to assure that they have not been altered; All correspondence with clients may be saved with dates of transmission / receipt; In case the company changes / upgrades its email or other systems, the new system should be able to read the old data and retain all data without change etc.

Question 3

ABC Industries Ltd., a company engaged in a business of manufacture and supply of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments.

The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to maintain continuity of business plans even while continuing the progress towards e-governance.

(a) What are the types of operations into which the different office activities can be broadly grouped under office automation systems?

(b) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity.

Answer

(a) Types of Operations:

The types of operations into which different office activities under Office Automation Systems can be broadly grouped, are discussed as under:

(i) **Document Capture:** Documents originating from outside sources like incoming mails from customers, enquiries, notes, handouts, charts, graphs etc. need to be preserved for being tracked through their life.

(ii) **Document Creation:** This consists of preparation of documents, editing of texts etc. and takes up major part of the time of field personnel like salesmen.

(iii) **Receipts and Distribution**: This basically includes distribution of correspondence to designated recipients. This may be effectively achieved by use of emails and mail groups.

(iv) **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time. E.g. categorizing various types of documents and cataloguing all documents under each type, assigning rights for access, retrieval

(v) **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.

(vi) **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation. Care should be taken to convert old documents which have not been created in or stored in computers into usable electronic documents so that after the new system is implemented, these old documents will still be accessible and business can continue as usual. Office automation systems which are already in use by some departments must be integrated with the new systems.

For e-governance, the company must put in place a definition of road map of how the systems will be implemented, monitored, measured and corrective action taken when deficiencies / opportunities for improvement are noticed. This will include assigning responsibilities to various personnel using or affected by office automation.

(b) Business Continuity Planning (BCP) is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. It is especially important because the company is planning to embrace office automation in all aspects of business. This will make it highly dependent on computer systems to run operations, deal with customers, suppliers and other stakeholders etc. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

(i) **Business Resumption Planning** – The Operational piece of business continuity planning to resume normal operations after a disaster.

(ii) **Disaster Recovery Planning** – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster. Planning which are minimal level of operations which must be run, their priority and the sequence in which they need to be brought up as well as taking steps to be prepared to deal with any emergency.

(iii) **Crisis Management** – The overall co-ordination of an organization’s response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization’s profitability, reputation or ability to operate. E.g. how to run operations and service customers when computer systems, are not available. The major international companies who have given orders to the company will expect this level of preparedness from the company.

Question 4

XYZ Industries Ltd., a company engaged in a business of manufacturing and supply of electronic equipments to various companies in India. It intends to implement E-Governance system at all of its departments. A system analyst is engaged to conduct requirement analysis and investigation of the present system. The company’s new business models and new *methods presume that the information required by the business managers is available all the time; it is accurate and reliable. The company is relying on Information Technology for information and transaction processing. It is also presumed that the company is up and running all the time on 24 x 7 basis. Hence, the company has decided to implement a real time ERP package, which equips the enterprise with necessary capabilities to integrate and synchronize the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. Also, the company intends to keep all the records in digitized form.*

(a) What do you mean by system requirement analysis? What are the activities to be performed during system requirement analysis phase?

(b) What is the provision given in Information Technology Act 2000 for the retention of electronic records?

Answer

(a) System requirements analysis is a phase, which includes a thorough and detailed understanding of the current system, identification of the areas that need modification/s to solve the problem, the determination of user/ managerial requirements and to have fair ideas about various system development tools.

The following activities are performed in this phase:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts e.g. what facilities the business owners require to gain competitive advantage; whether for meeting 24x7 requirements documents should be accessible over internet, whether customers and suppliers will also connect to the system;
- To analyze requirements to detect and correct conflicts and determine priorities; this will include identifying the various documents which will need to be migrated to the new system. In case the existing systems process transactions in a way different from the new ERP, these differences must be resolved
- To verify requirements in terms of various parameters like completeness, consistency, unambiguous, verifiable, modifiable, testable and traceable;
- To gather data or find facts using tools like- interviewing, research/document collection, questionnaires, observation;
- To develop models to document Data Flow Diagrams, E-R diagrams; and
- To develop a system dictionary to document the modeling activities.
- The document/deliverable of this phase is a detailed system requirements report, which is generally termed as SRS.

(b) **Retention of Electronic Records: [Section 7] of Information Technology Act 2000:** The provision for the retention of electronic records is discussed in Section 7 of IT Act 2000, which is given as follows:

(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;

(c) 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.

E.g. Company may include clause in its contracts with customers that electronic documents and correspondence will be considered valid; Electronic documents will have to be preserved till the contract and all liabilities are discharged; Documents may be digitally signed with hash values to assure that they have not been altered; All correspondence with clients may be saved with dates of transmission / receipt; In case the company changes / upgrades its email or other systems, the new system should be able to read the old data and retain all data without change etc.

Question 5

ABC Technologies Ltd. is in the development of web applications for various domains. For the development purposes, the company is committed to follow the best practices suggested by SDLC. A system development methodology is a formalized, standardized, documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations.

Read the above carefully and answer the following:

(a) Describe accountants' involvement in development work in brief.

(b) 'Waterfall approach is one of the popular approaches for system development'. Explain the basic principles of this approach.

(c) Briefly describe major characteristics of Agile Methodology.

Answer

(a) Accountants' involvement in Development work: An accountant can help in various related aspects during system development; some of them are as follows:

(i) Return on Investment (referred as RoI): This calculates the return an entity shall earn on a particular investment i.e. capital expenditure. This financial data is a prime consideration for evaluating any capital expenditure by the entity. The important data required for this analysis are the cost of implementing and running the project, and the expected revenue/ benefit for a given period. The analysis ideally needs to be done before the start of the development efforts for better decision making by management. For this analysis following data needs to be generated.

(1) **Cost:** This includes estimates for typical costs involved in the development, which are given as follows:

- **Development Costs:** Development Costs for a computer based information system include costs of the system development process, like salaries of developers, software, equipment depreciation etc.
- **Operating Costs:** Operating Costs of a computer based information system including hardware/ software rental or depreciation charges; salaries of computer operators and other data processing personnel, who will operate the new system.
- **Intangible Costs:** Intangible Costs that cannot be easily measured. For example, the development of a new system may disrupt the activities of an organization and cause a loss of employee productivity or morale.

(2) **Benefits:** The benefits, which result from developing new or improved information systems can be subdivided into tangible and intangible benefits. A post implementation analysis is also done to see how the system development effort has benefitted an organization. For example: A large oil company in public sector, implemented an ERP system few years back at a total cost of ` 100 crores. The calculated benefits from the project were ` 40 crores per annum. Above data gives an RoI of 40%, which is tremendous for any business. It also tells that the payback period is around 2.5 years.

(ii) Computing Cost of IT Implementation and Cost Benefit Analysis: For analysis of ROI, accountants need the costs and returns from the system development efforts. For correct generation of data, proper accounting needs to be done. Accountants are the persons to whom management look for this purpose.

(iii) Skills expected from an Accountant: An accountant, being an expert in accounting field must possess skills to understand the system development efforts and nuances of the same. S/he is expected to have various key skills, including understanding of the business objectives, expert book keeper, and understanding of system development efforts etc.

(b) Basic Principles of Waterfall Approach: Major principles of Waterfall approach are given as follows:

♦ Project is divided into sequential phases, with some overlap and splash back acceptable between phases.

- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/ signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

(c) Major characteristics of Agile Methodology are as follows:

- Customer satisfaction by rapid delivery of useful software;
- Welcome changing requirements, even late in development;
- Working software is delivered frequently (in weeks rather than months);
- Working software is the principal measure of progress;
- Sustainable development, able to maintain a constant pace;
- Close, daily co-operation between business people and developers;
- Face-to-face conversation is the best form of communication (co-location);
- Projects are built around motivated individuals, who should be trusted;
- Continuous attention to technical excellence and good design;
- Simplicity; Self-organizing teams; and
- Regular adaptation to changing circumstances.

Question 6

ABC Group of Industries is in the process of launching a new business unit, ABC Consultants Ltd. to provide various consultancy services to the organizations worldwide, to assist them in the computerization of their business modules. It involves a number of activities starting from capturing of requirements to maintenance. Business continuity and disaster recovery planning are two key activities in this entire process, which must be taken care of right from the beginning. Business continuity focuses on maintaining the operations of an organization, especially the IT infrastructure in face of a threat that has materialized. Disaster recovery, on the other hand, arises mostly when business continuity plan fails to maintain operations and there is a service disruption. This plan focuses on restarting the operations using a prioritized resumption list.

Read the above carefully and answer the following:

(a) What are the issues, which are emphasized by the methodology for developing a business continuity plan?

(b) Explain the objectives of performing Business Continuity Planning tests.

(c) What are the issues, written in a contract that should be ensured by security administrators if a third-party site is to be used for recovery purposes?

Answer

(a) The methodology for developing a business continuity plan emphasizes the following:

(i) Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;

(ii) Obtaining commitment from appropriate management to support and participate in the effort;

(iii) Defining recovery requirements from the perspective of business functions;

(iv) Documenting the impact of an extended loss to operations and key business functions;

(v) Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;

(vi) Selecting business continuity teams that ensure the proper balance required for plan development;

(vii) Developing a business continuity plan that is understandable, easy to use and maintain;

(viii) Planning the testing of plans in a systematic manner and measuring results of such tests; and

(ix) Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.

(b) The objectives of performing BCP tests are to ensure that:

- the recovery procedures are complete and workable.
- the competence of personnel in their performance of recovery procedures can be evaluated.
- the resources such as business processes, IS systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
- manual recovery procedures and IT backup system/s are current and can either be operational or restored.
- the success or failure of business continuity training program is monitored.

(c) If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover issues such as:

- how soon the site will be made available subsequent to a disaster,
- the number of organizations that will be allowed to use the site concurrently in the event of a 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 the site can be used.
- the facilities and services the site provider agrees to make available,
- procedures to ensure security of company's data from being accessed / damaged by other users of the facility and
- what controls will be in place for working at the off-site facility.

Question 7

ABC Technologies Ltd. deals with the software developments for various domains. The company is following SDLC best practices for its different activities. For any software to be developed, after possible solutions are identified, project feasibility i.e. the likelihood that the system will be useful for the organization, is determined. After this, other stages of the SDLC are followed with their best practices. A system development methodology is a formalized, standardized, documented set of activities used to manage a system development project. It refers to the framework that is used to structure, plan and control the process of developing an information system. Each of the available methodologies is best suited to specific kinds of projects, based on various technical, organizational, project and team considerations.

Read the above carefully and answer the following:

(a) What is a feasibility study? Explain the dimensions under which the feasibility study of a system is evaluated.

(b) For the development of software, various techniques/models are used e.g. waterfall, incremental, spiral etc; in which, each has some strengths and some weaknesses. Discuss the weaknesses of the incremental model.

Answer

(a) A feasibility study is carried out by system analysts, which refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The Feasibility Study of a system is evaluated under following dimensions:

- **Technical:** Is the technology needed available?
- **Financial:** Is the solution financially viable?
- **Economic:** What is the Return on Investment?
- **Schedule/Time:** Can the system be delivered on time?
- **Resources:** Are human resources available to develop the solution or are they reluctant to use it ?

- **Operational:** How will the solution work?
- **Behavioral:** Is the solution going to bring any positive or adverse effect on quality of work life?
- **Legal:** Is the solution valid in legal terms?

(b) Major weaknesses of the incremental model are given as follows:

- When utilizing a series of mini-waterfalls for a small part of the system before moving onto the next increment, there is usually a lack of overall consideration of the business problem and technical requirements for the overall system.
- Each phase of iteration is rigid and does not overlap each other.
- Problems may arise pertaining to system architecture because not all requirements are gathered up front for the entire software life cycle.
- Since some modules will be completed much earlier than others, hence well-defined interfaces are required.
- Difficult problems tend to be pushed to the future to demonstrate early success to management.

Question 8

ABC Ltd. is a company dealing in various computer hardware items through its various offices in India and abroad. By recognizing the advantages of connectivity through internet, recently, the company decided to sell its products in on-line mode also to facilitate its customers worldwide. For development of the company's web applications, the company appointed a technical consultant initially for one year to work on behalf of the company to take the matter forward. The consultant called various meetings of different stakeholders and decided to follow the best practices of SDLC for its different phases. In the current vulnerable world, keeping the importance of information security in view particularly, he further suggested to consider the security issues from the inception itself i.e. starting from the requirements analysis phase till maintenance. Accordingly, efficient ways were also explored to achieve the goals especially for security. Research Studies reveal that cost and efforts may be reduced up to a considerable level by incorporating security from the beginning in the SDLC.

Read the above carefully and answer the following:

(a) What is SDLC? Explain the key activities performed in the Requirements Analysis phase.

(b) Agile methodology is one of the popular approaches of system development. What are the weaknesses of this methodology in your opinion?

Answer

(a) System Development Life Cycle (SDLC) framework provides system designers and developers a sequence of activities to follow. It consists of a set of steps or phases in which each phase of the SDLC uses the results of the previous one. The SDLC is document driven, which means that at crucial stages during the process, documentation is produced. A phase of the SDLC is not complete until the appropriate documentation or artifact is produced. These are sometimes referred as deliverables.

Key activities, which are performed in the 'Requirements Analysis Phase', are given as follows:

- To identify and consult the stakeholders to determine their expectations and resolve their conflicts;
- To analyze requirements to detect and correct conflicts and determine priorities;
- To verify the requirements to be 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; and
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

(b) Major weaknesses of agile methodology are given as follows:

- In case of some software deliverables, especially the large ones, it is difficult to assess the efforts required at the beginning of the software development life cycle. Hence, appropriate resources may not be available or cost-benefit may be overestimated.
- There is lack of emphasis on necessary design and documentation. This makes maintenance difficult.
- Agile increases potential threats to business continuity and knowledge transfer. By nature, Agile projects are extremely light on documentation because the team focuses on verbal communication with the customer rather than on documents or manuals.
- Agile requires more re-work. Because of the lack of long-term planning and the lightweight approach to architecture, re-work is often required on Agile projects when the various components of the software are combined and forced to interact.
- The project can easily get taken off track if the customer representative is not clear about the final outcome that they want.
- Only senior programmers are capable of taking the kind of decisions required during the development process. Hence, it has no place for newly appointed programmers, unless combined with experienced resources.
- Agile lacks the attention to outside integration. Because Agile teams often do not invest the time in identifying and designing the integration points with other systems in advance, the need for an integration point can become a last-minute surprise that often requires re-work, additional time, removal from scope, or a poor-quality product.

Question 9

XYZ Limited is a multinational company engaged in providing financial services worldwide. Most of the transactions are done online. Their current system is unable to cope up with the growing volume of transactions. Frequent connectivity problems, slow processing and a few instances of phishing attacks were also reported. Hence the Company has decided to develop a more robust in-house software for providing good governance and sufficient use of computer and IT resources. You, being an IS auditor, has been appointed by the Company to advise them on various aspects of project development and implementation. They want the highest levels of controls in place to maintain data integrity and security with zero tolerance to errors.

The Company sought your advise on the following issues:

(a) What are the major data integrity policies you would suggest?

(b) What are the categories of tests that a programmer typically performs on a program unit?

(c) Discuss some of the critical controls required in a. computerized environment.

(d) What are your recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing'? \\

Answer

(a) Major data integrity policies are given as under:

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

(b) There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

- *Functional Tests: Functional Tests check 'whether programs do, what they are supposed to do or not'. The test plan specifies operating conditions, input* *values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.*

- *<u>Performance Tests:</u> Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.*
- *<u>Stress Tests:</u> Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. The purpose of a stress test is to determine the limitations of the program.*
- *<u>Structural Tests:</u> Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.*
- *<u>Parallel Tests:</u> In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.*

(c) Some of the critical controls required in a computerized environment are as follows:

- *Management understanding of Information System risks and related controls;*
- *Presence or adequate Information System control framework;*
- *Presence of general controls and Information System controls;*
- *Awareness and knowledge of Information System 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 adequate security functionality in technologies implemented.*

(d) Some recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing' are as follows:

- *Power-down the CPU and all peripherals during extended periods of inactivity.*
- *Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.*
- *Power-up and power-down energy-intensive peripherals such as laser printers according to need.*

- *Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.*
- *Use notebook computers rather than desktop computers whenever possible.*
- *Use the power-management features to turn off hard drives and displays after several minutes of inactivity.*
- *Minimize the use of paper and properly recycle waste paper.*
- *Dispose of e-waste according to central, state and local regulations.*
- *Employ alternative energy sources for computing workstations, servers, networks and data centers.*

Question 10

E-quip Limited has worldwide operations and is engaged in the business of manufacturing and supply of electronic equipment through its various outlets in India and abroad. Recognizing the advantages of connectivity through internet, the Management decides to sell its products in on-line mode by using Cloud Computing technology to achieve this objective.

The Company appoints a technical team for the development of the Company's new web application. The team calls for various meetings of different stakeholders and decides to follow the best practices of SDLC for its different phases. Keeping the importance of information security in the current vulnerable world, it suggests that security issues must be considered from the beginning itself. Accordingly, Business Impact Analysis (BIA) was done as a part of Business Continuity Management (BCM). As the auditor member of the technical team, the Management of E-quip Limited wants you to advise them on the following issues:

(a) What are the advantages and important implications of the proposed Information System for the Company?

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

(c) Management wants to know the major challenges in using Cloud Computing technology for running the new web application. Write any five challenges.

(d) Explain briefly major ways to control remote and distributed data processing in the new Web Application.

Answer

(a) The major advantage of the proposed Information system will be that it will enable the E-quip Limited to sell its products in an online mode in India and abroad through Internet connectivity by using Cloud Computing Technology. The proposed Information system will support company's business processes and operations; better business decision making; and will provide strategic and

competitive advantage to ensure better quality and supply of its electronic equipments.

Following are some of the important implications of proposed Information Systems in business for E-Quip Limited:

- *Information system helps managers in efficient decision-making to achieve the organizational goals.*
- *An organization will be able to survive and thrive in a highly competitive environment on the strength of a well-designed Information system.*
- *Information systems helps in making right decision at the right time i.e. just on time.*
- *A good information system may help in generating innovative ideas for solving critical problems.*
- *Knowledge gathered though Information system may be utilized by managers in unusual situations.*
- *Information system is viewed as a process; it can be integrated to formulate a strategy of action or operation.*

(b) 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.*

(c) Major challenges in Cloud Computing Technology for running new Web application are as follows:

- ***Confidentiality:*** ***Prevention of the unauthorized disclosure of the data is referred as Confidentiality. With the use of encryption and physical isolation, data can be kept secret.***
- ***Integrity:*** ***Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible.***
- ***Availability:*** ***Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure and natural calamities are all threats to availability.***
- ***Governance:*** ***Due to the lack of control over the employees and services, there is problem relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization.***
- ***Trust:*** ***Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.***
- ***Legal Issues and Compliance:*** ***There are various types of laws and regulations that impose security and privacy duties on the organization and potentially impact Cloud computing initiatives such as demanding privacy, data location and security controls, records management, and E-discovery requirements.***
- ***Privacy:*** ***The privacy issues are embedded in each phase of the Cloud design that includes both the legal compliance and trusting maturity.***
- ***Audit:*** ***Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'.***
- ***Data Stealing:*** ***In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. Some of the Cloud providers use server/s from other service providers and thus there is a probability that the data is less secure and is more prone to the loss from external server.***
- ***Architecture:*** ***In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The reliability and scalability of architecture is dependent on the design and implementation to support the overall framework.***
- ***Identity Management and Access control:*** ***A robust federated identity management architecture and strategy internal in the organization provides a***

trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.

- *<u>Incident Response:</u> It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.*
- *<u>Software Isolation:</u> Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture and evaluate the risks required for the organization.*
- *<u>Application Security:</u> Security issues relating to application security still apply when applications move to a cloud platform. Service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server.*

(d) Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

- *Remote access to computer and data files through the network should be implemented.*
- *Having a terminal lock can assure physical security to some extent.*
- *Applications that can be remotely accessed via modems and other devices should be controlled appropriately.*
- *Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.*
- *In order to prevent the unauthorized users' access to the system, there should be proper control mechanisms over system documentation and manuals.*
- *Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.*
- *When replicated copies of files exist at multiple locations, it must be ensured that all are identical copies that contain the same information and checks are also done to ensure that duplicate data does not exist.*

FEEDBACK FORM

(1)	Name of the Student	
(2)	Registration No.	
	Contact detail with e-mail id, mobile number, etc.	
(3)	Subject & Paper No.	PAPER: 6 : Information Systems Control and Audit
(4)	Name of Publication	Practice Manual
(5)	Edition	January, 2016
(6)	Do you find the publication student-friendly?	
(7)	Do the illustrations in the Study Material assist in understanding of the provisions contained in the Study Material?	
(8)	Does the Practice Manual contain adequate and sufficient questions to help in better understanding of the concepts explained in the Study Material?	
(9)	Are there any errors which you have noticed in the publication? If yes, give the specific details :	

	Type of Error (Specify nature of error)	Chapter No. (Unit No., if applicable)	Page No.	Para No. & line of the para	Text or problem (containing the error) as per the publication	Suggested Correction
	Typographical/ Printing/ Computational/ Conceptual/ Updation					
(10)	Do you feel that the publication can be made more value additive? If so, please give your specific suggestions. ____ ____					

Note: Use separate sheet if necessary. You are also encourage to send response by e-mail on feedbackbos@icai.org

Please send feedback form to :

Director Board of Studies
The Institute of Chartered Accountants of India
A-29, Sector-62, Noida- 201 309.