Test Series: May, 2020

MOCK TEST PAPER 1

FINAL COURSE GROUP - II

PAPER - 6: INFORMATION SYSTEMS CONTROL AND AUDIT

ANSWERS

Part I: Multiple Choice Questions

1. **(b)** Section 43A
2. **(a)** Cloud Computing
3. **(b)** Salami Technique
4. **(d)** The frequency for which the site provider agrees to make itself available for a particular time period.
5. **(b)** Office Automation System
6. **(c)** Understanding of system development methodologies
7. **(b)** The numbers of management levels are fixed to three irrespective of its size and structure.
8. **(b)** (iv)-(i)-(v)-(ii)-(vi)-(iii)
9. **(d)** Mitigating the risk
10. **(a)** Software Component, Process Flow, Customer mindset, Change Management
11. **(c)** Piggybacking is defined as an act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions.
12. **(c)** Differential backups are faster than Incremental backups.
13. **(c)** Adaptive Maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system.
14. **(d)** According to SA-234, Audit Documentation refers to the record of audit procedures performed, relevant audit obtained and conclusions the auditor reached.
15. **(b)** Addressee means a person including intermediary who is intended by the originator to receive the electronic record.
16. **(a)** As the complete cloud is being shared by several organizations or community, it becomes highly expensive.
17. **(d)** The GRC framework which has been a regulatory requirement not only for listed enterprises but also for all types of enterprises stands for Governance, Risk and Control.
18. **(b)** MIS cannot be implemented without using a computer.
19. **(a)** The surprise check of raw materials stock by a supervisor in a manufacturing company is an example of Corrective Control.
20. **(c)** Likelihood, Consequences
21. **(d)** Alpha Testing
22. **(d)** Scoping, Planning, Fieldwork, Analysis, Reporting, Close

Part II: Descriptive Questions

1. (a) The key principles of COBIT 5 are as follows:

- **Principle 1 - Meeting Stakeholder Needs:** Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

  The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals; IT related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

- **Principle 2 - Covering the Enterprise End-to-End:** COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. It considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e. inclusive of everything and everyone - internal and external that is relevant to governance and management of enterprise information and related IT.

- **Principle 3 - Applying a Single Integrated Framework:** There are many IT related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

- **Principle 4 - Enabling a Holistic Approach:** Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.

- **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.

(b) Various risks related to Personal Computers (PC) 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.
- Most of the log-on procedures become active only at the booting of the computer from the hard drive.

The security measures that could be exercised to overcome these aforementioned risks are 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;
- The use of personal computer and their peripheral must have controls; and
- Use of disc locks that prevent unauthorized access to the floppy disk or pen drive of a computer.

(c) The factors that are responsible to influence an organization towards control and audit of its computers are as follows:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.).
- **Value of Computer Hardware, Software and Personnel***:* These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
- **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

2. (a) Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. The Auditor should verify:

- The IPF (Infrastructure Planning and Facilities) and the construction with regard to the type of materials used for construction;
- The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;

- The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
- Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly fire drill to test the preparedness;
- Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors;
- Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment and generators. Also the power supply interruptions must be checked to test the effectiveness of the back-up power;
- Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc;
- Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair) are within acceptable levels; and
- Identify undesired activities such as smoking, consumption of eatables etc.

(b) There are various kinds of plans that need to be designed as a part of Business Continuity Management (BCM). They include the following:

- **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.

  When the situations that evoke 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 designated. In all cases, the personnel responsible for the actions must be identified and the protocols to be followed must be specified clearly.

- **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. For some resources, the procedures specified in the backup plan might be straightforward. In other cases, the procedures specified in the backup plan could be complex and somewhat uncertain. The backup plan needs continuous updating as changes occur. For example, as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly. Indeed, it is prudent to have more than one person knowledgeable in a backup task in case someone is injured when a disaster occurs. Similarly, lists of hardware and software must be updated to reflect acquisitions and disposals.

- **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.

- **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.

  To facilitate testing, a phased approach can be adopted. First, the disaster recovery plan can be tested by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs. Next, a disaster can be simulated at a convenient time- for example, during a slow period in the day. Anyone, who will be affected by the test (e.g. personnel and customers) also, might be given prior notice of the test so they are prepared. Finally, disasters could be simulated without warning at any time. These are the acid tests of the organization's ability to recover from a catastrophe.

(c) **Segregation of Duties:** Segregation of Duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose is to prevent or detect errors or irregularities by applying suitable controls. It reduces the likelihood of errors and wrongful acts going undetected because the activities of one group or individual will serve as a check on the activities of the other. The irregularities are frauds due to various facts like Theft of assets like funds, IT equipment, the data and programs; Modification of the data leading to misstated and inaccurate financial statements; and Modification of programs in order to perpetrate irregularities like rounding down, salami etc.

Examples of Segregation of Duties are as follows:

- Systems software programming group from the application programming group;
- Database administration group from other data processing activities;
- Computer hardware operations from the other groups;
- Systems analyst function from the programming function;
- Physical, data, and online security group(s) from the other IS functions; and
- IS Audit from business operations groups.

From a functional perspective, segregation of duties should be maintained between the Information systems use; Data entry; Computer operation; Network management; System administration; Systems development and maintenance; Change management; Security administration, and Security audit.

3. **(a)** Information Systems are categorized as follows:

(i) **Operational-Level Systems:** These support operational managers in tracking elementary activities. These can include tracking customer orders, invoice tracking, etc. Operational-level systems or Operational Support Systems (OSS) ensure that business procedures are followed. Information systems are required to process the data generated and used in business operations. OSS produces a variety of information for internal and external use. Its 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. Example – Transaction Processing System (TPS) is an operational level system.

(ii) **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. It helps the organization's knowledge and data workers and is especially in the form of workstations. It is the fastest growing application in business today. Example - Office Automation Systems (OAS) and Knowledge Management systems.

(iii) Management-Level Systems: These support the middle managers in monitoring, decision-making and administrative activities and are helpful in answering questions like - Are things working well and in order? These provide 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 types of systems mainly answer "what if" questions. For example - What would be quality of teaching if college has to achieve top ranking in academics? These types of questions can be answered only after getting new data from outside the organization, as well as data from inside which cannot be easily obtained from existing operational level systems.

MSS supports managers in effective decision making by providing relevant and required information at the right time to the right people. Management Information System and Decision Support Systems are types of Management Level systems.

(iv) Strategic Level Systems: These systems are for strategic managers to track and deal with strategic issues, assisting long-range planning. These systems support the senior level management to tackle and address strategic issues and long term trends, both inside organization and the outside world. These answer questions like what products should be launched to increase the profit and capture the market. It helps in long term planning. A principle area is tracking changes in the external conditions (market sector, employment levels, share prices etc.) and matching these with the internal conditions of the organization. For example - Executive Information Systems (EIS) also referred as Executive Support System (ESS).

(b) The following are some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review.

(i) Knowledge of the Business: Related aspects are given as follows:

- General economic factors and industry conditions affecting the entity's business,
- Nature of Business, its products & services,
- General exposure to business,
- Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced,
- Level of competence of the Top management and IT Management, and
- Finally, Set up and organization of IT department.

(ii) Understanding the Technology: An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on 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.

(iii) Understanding Internal Control Systems: For gaining understanding of Internal Controls emphasis is to be placed on compliance and substantive testing.

(iv) Legal Considerations and Audit Standards: Related points are given as follows:

- The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work.
- The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
- The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organization. Sometimes, this may also include restrictions on the use of certain types of technologies e.g. freeware, shareware etc.
- The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

(v) Risk Assessment and Materiality: Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation. It implies the process of identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence. Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk (the risk of errors occurring in the area being audited). Additionally, risk assessment will aid in planning decisions such as nature, extent, and timing of audit procedures; the areas or business functions to be audited, and the amount of time and resources to be allocated to an audit.

Risks that affect a system and taken into consideration at the time of assessment can be differentiated as inherent risks, control risks and detection risks. These factors directly impact upon the extent of audit risk which can be defined as the risk that the information/financial report may contain material error that may go undetected during the course of the audit. At this stage, the auditor needs to assess the expected inherent, control and detection risk and identify significant audit areas; set materiality levels for audit purposes and assess the possibility of potential vulnerabilities, including the experience of past periods, or fraud.

(c) Section 65 of information Technology Act, 2000 is as follows:

[Section 65] Tampering with Computer Source Documents

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.

4. (a) The limitations of Mobile Computing are as follows:

- **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and Enhanced Data for GSM (Global System for Mobile Communication) Evolution (EDGE), and more recently 3G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.
- **Security Standards:** When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards. One can easily attack the VPN through a huge number of networks interconnected through the line.
- **Power consumption:** When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.
- **Transmission interferences:** Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.
- **Potential health hazards:** People who use mobile devices while driving are often distracted from driving are thus assumed to be more likely involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.
- **Human interface with device:** Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

(b) **Corrective Controls** are the controls that 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.

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.

Some of the Corrective Controls may be Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system; and Investigate budget variance and report violations.

(c) The maintenance tasks undertaken in development of Business Continuity Plan (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.

5. (a) Regarding Audit, SEBI has 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 atleast 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.

(b) Information Systems Audits has been categorized into following five types:

(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.

(c) Program Debugging is the most primitive form of testing activity, which refers to correcting programming language syntax and diagnostic errors so that the program compiles cleanly. A clean compile means that the program can be successfully converted from the source code written by the programmer into machine language instructions. Debugging can be a tedious task consisting of following four steps:

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

6. (a) Detailed investigation of the present system involves collecting, organizing and evaluating facts about the system and the environment in which it operates for which following areas should be studied in depth:

- **Reviewing Historical Aspects:** A brief history of the organization is a logical starting point for an analysis of the present system. The historical facts enable to identify the major turning points and milestones that have influenced its growth. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments. The system analyst should investigate 'what system changes have occurred in the past including operations' that have been successful or unsuccessful with computer equipment and techniques.
- **Analyzing 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 various sources from where the data are 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, s/he will be able to determine how these inputs fit into the framework of the present system.
- **Reviewing Data Files:** The analyst 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 on-line and off-line files, which are maintained in the organization as it will reveal information about data that are not contained in any outputs. The related cost of retrieving and processing the data is another important factor that should be considered by the systems analyst.
- **Reviewing 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 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. S/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.

- **Analyzing 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 carry-over from earlier days and have little relevance to current operations. Attempts should be made to eliminate all such reports in the new system.
- **Reviewing Internal Controls:** A detailed investigation of the present information system is not complete until internal control mechanism is 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 controls may indicate weaknesses that should be removed in the new system. The adoption of advanced methods, procedures and equipments might allow much greater control over the data.
- **Modeling the Existing System:** As the logic of inputs, methods, procedures, data files, data communications, reports, internal controls and other important items are reviewed and analyzed in a top down manner; the processes must be properly documented. The flow charting and diagramming of present information not only organizes the facts, but also helps to disclose gaps and duplication in the data gathered. It allows a thorough comprehension of the numerous details and related problems in the present operation.
- **Undertaking Overall Analysis of the Existing 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 costs-benefits of each of these must be investigated thoroughly.

(b) The key management practices, which are required for aligning IT strategy with enterprise strategy, are 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. These 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.

(c) The competence of an IS Auditor as suggested by Reserve Bank of India (RBI) is as follows:

- IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience. They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training.
- As IT encompasses a wide range of technologies, IS Auditors should possess skills that are commensurate with the technology used by a bank. They should be competent audit professionals with sufficient and relevant experience.
- Qualifications such as Certified Information Systems Auditor, Information Systems Audit or Certified Information Systems Security Professional along with two or more years of IS Audit experience, are desirable. Similar qualification criteria should also be insisted upon, in case of outsourced professional service providers.