PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

Candidates are also required to answer any five questions

from the remaining six questions.

Question 1

Bharat Bank (BB) is a large bank with more than 3000 branches and 15000 ATMs in India. With an aim to grow further, it has acquired three smaller private banks with similar lines of business. This acquisition has brought a variety of products, applications and branches under its umbrella. Besides consumer banking through brick and mortar branches, BB also wants to consolidate its position through internet banking.

The growth strategy of the bank has resulted in fragmented business operations that operate in a regional structure as well as a disjoint IT environment. Hence BB wishes to implement a new, cutting edge web based Core Banking System to manage all its operations from a single window. BB also recognizes that failure or malfunction of any critical system will cause significant operational disruptions and materially impact its ability to provide service to its customers. To overcome this risk, BB plans to implement Business Continuity Management (BCM). You have been appointed by BB to make a presentation to the Board of Directors to justify the need for the new system. Please answer the following queries raised by the Management:

(a) What are the key management practices which are required for aligning IT Strategy of BB with its Enterprise Strategy? (5 Marks)

(b) What are the IT tools you consider critical for business growth ? (5 Marks)

(c) What are the suggested system controls that should be covered under IS audit as per the requirement of the Reserve Bank of India? (5 Marks)

(d) Explain the five stages or components of the BCM process which will help BB to manage any future disruptions of the proposed new Core Banking System. (5 Marks)

Answer

(a) The key management practices which are required for aligning IT strategy of Bharat Bank (BB) with its 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. 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.

(b) Some of the IT tools critical 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 – Through Internet, 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.

(c) The System Controls that should be covered under the Information Systems' audit as per the requirement of the Reserve Bank of India (RBI) are as follows:

- Duties of system programmer/designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming/design. System person would only make modifications/improvements to programs and the operating persons would only use such programs without having the right to make any modifications.
- Contingency plans/procedures in case of failure of system should be introduced/ tested at periodic intervals. EDP auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.
- An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements.
- In order to bring about uniformity of software used by various branches/offices, there should be a formal method of incorporating change in standard software and it should be approved by senior management. Inspection and Audit Department should verify such changes from the view-point of control and for its implementation in other branches in order to maintain uniformity.
- Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively.
- There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
- With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, at least once every three years, on the banks Internal Audit including IS Audit to validate the approach and practices

adopted by them in the discharge of its responsibilities as laid out in the Audit Charter/Audit Policy.

(d) The stages or components of the BCM process which will help Bharat Bank (BB) to manage any future disruptions of the proposed new Core Banking system are as follows:

- Stage 1: BCM – Information Collection Process: The activities of assessment process do the prioritization of an enterprise's products and services and the urgency of the activities that are required to deliver them. This sets the requirements that will determine the selection of appropriate BCM strategies in the next process.
- Stage 2: BCM – Strategy Process: Finalization of business continuity strategy requires assessment of a range of strategies. This requires an appropriate response to be selected at an acceptable level and during and after a disruption within an acceptable timeframe for each product or service, so that the enterprise continues to provide those products and services. The selection of strategy will take into account the processes and technology already present within the enterprise.
- Stage 3: BCM – Development and Implementation Process: This deals with the development of a management framework and a structure of incident management, business continuity and business recovery and restoration plans.
- Stage 4: BCM – Testing and Maintenance Process: BCM testing, maintenance and audit testify the enterprise BCM to prove the extent to which its strategies and plans are complete, current and accurate; and identifies opportunities for improvement.
- Stage 5: BCM – Training Process: Extensive trainings in BCM framework, incident management, business continuity and business recovery and restoration plans enable it to become part of the enterprise's core values and provide confidence in all stakeholders in the ability of the enterprise to cope with minimum disruptions and loss of service.

Question 2

(a) Operating System not only provides the platform for an application to use various IS resources but is also the last barrier to be conquered for unlimited access to all the resources. Explain the statement by describing any six operating system access controls to protect IS resources from unauthorised access. (6 Marks)

(b) Cloud Computing service providers offer their services on the lines of several fundamental models. Describe the various types of Cloud Computing models. (6 Marks)

(c) Discuss the factors to be considered to validate a vendor's proposal at the time of software acquisition. (4 Marks)

Answer

(a) Operating system not only provides the platform for an application to use various Information System resources but is also the last barrier to be conquered for unlimited access to all the resources. Hence, protecting operating system access is extremely crucial. Some of the common operating system access controls to protect IS resources from unauthorized access are as follows:

- Automated terminal identification: This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.
- Terminal log-on procedures: The log-on procedure does not provide unnecessary help or information, which could be misused by an intruder.
- User identification and authentication: The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
- Password management system: An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
- Use of system utilities: System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
- Duress alarm to safeguard users: If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.
- Terminal time out: Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
- Limitation of connection time: Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m.—or on a Saturday or Sunday.

(b) Cloud Computing service providers offer their services on the lines of several fundamental models. Various types of Cloud Computing Models are as follows:

- 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. In order to deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure. Examples of IaaS providers include: Amazon EC2, Azure Services Platform, Dyn DNS, Google Compute Engine, HP Cloud etc.

- Platform as a Service (PaaS): Cloud providers deliver a computing platform including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of acquiring and managing the underlying hardware /software layers. In PaaS, one can make applications and software's on other's database. Thus, it gives us the platform to create, edit, run and manage the application programs we want. All the development tools are provided. Some of examples of PAAS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard etc.
- Software as a Service (SaaS): SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning software as a service.
- 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. Some of the examples are Virtual Private Network, Mobile Network Virtualization etc.
- 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 vender. 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 the large capital investments. Examples are Voice over IP (VoIP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.

(c) The contracts and software licensing process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming. The following factors have to be considered to validate a vendors' proposal at the time of software acquisition:

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

Question 3

(a) Maintaining the system is an important aspect of system development. Elaborate the various categories of system maintenance. (6 Marks)

(b) ABC Ltd. is looking for a suitable IS auditor. Please send an introductory note to ABC Ltd. explaining your suitability by describing the skill set and competence you possess for the job other than your qualification. (6 Marks)

(c) ABC Ltd. is not aware of the importance and requirement relating to 'Retention of Electronic Records' as per IT Act, 2008. Please enlighten them on this. (4 Marks)

Answer

(a) Maintaining the system is an important aspect of System Development. Maintenance can be categorized in the following ways:

- Scheduled Maintenance: Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- Rescue Maintenance: Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- Corrective Maintenance: Corrective maintenance deals with fixing bugs in the code or defects found during the executions. 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 the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or 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 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.
- 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. The long-

term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

(b) ABC Ltd. is looking for a suitable IS auditor. I hereby explain my suitability for the same, as I hereby announce that I possess the desired skill set that is generally expected to be with an IS auditor which includes the following:

- Sound knowledge of business operations, practices and compliance requirements;
- 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.
- 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.

(c) As per IT Act, 2008, "Section 7 deals with Retention of Electronic Records". The Section provides that -

(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, if -

(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:

PROVIDED that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Question 4

(a) Describe how the application controls and their audit trail are categorised. (6 Marks)

(b) Describe the prototyping model of system development explaining the generic phases of this model. (6 Marks)

(c) Describe the major components of Web 2.0 for social networks. (4 Marks)

Answer

(a) The Application Controls are categorized as below:

- Boundary Controls: Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.
- Input Controls: These are responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.
- Communication Controls: These are 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: These are 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.
- Output Controls: These are the 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.
- Database Controls: These are 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.

  The following two types of Audit Trail controls should exist in each application control:

  - An Accounting Audit Trail to maintain a record of events within the subsystem; and
  - An Operations Audit Trail to maintain a record of the resource consumption associated with each event in the subsystem.

(b) The traditional approach to develop a system sometimes may take years to analyze, design and implement a system. More so, many a times we know a little about the system until and unless we go through its working phases, which are not available. In

order to avoid such bottlenecks and overcome the issues, organizations are increasingly using prototyping techniques to develop smaller systems such as Decision Support System, Management Information System, and Expert systems. The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system.

A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of 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 the 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 it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

The generic phases of Prototyping model of a system development are as follows:

- Identify Information System Requirements: In traditional approach, the system requirements are to be identified before the development process starts. However, under prototype approach, the design team needs only fundamental system requirements to build the initial prototype, the process of determining them can be less formal and time -consuming than when performing traditional systems analysis.
- Develop the Initial Prototype: The designers create an initial base model and give little or no consideration to internal controls, but instead emphasize system characteristics such as simplicity, flexibility, and ease of use. These characteristics enable users to interact with tentative versions of data entry display screens, menus, input prompts, and source documents. The users also need to be able to respond to system prompts, make inquiries of the information system, judge response times of the system, and issue commands.
- Test and Revise: After finishing the initial prototype, the designers first demonstrate the model to users and then give it to them to experiment and ask users to record their likes and dislikes about the system and recommend changes. Using this feedback, the design team modifies the prototype as necessary and then resubmits the revised model to system users for reevaluation. Thus iterative process of modification and reevaluation continues until the users are satisfied.
- Obtain User Signoff of the Approved Prototype: Users formally approve the final version of the prototype, which commits them to the current design and establishes a contractual obligation about what the system will, and will not, do or provide. Prototyping is not commonly used for developing traditional applications such as accounts receivable, accounts payable, payroll, or inventory management, where the inputs, processing, and outputs are well known and clearly defined.

(c) Major components that have been considered in Web 2.0 include the following:

- Communities: These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are a number of tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.
- Blogging: Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.
- Wikis: A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.
- Folksonomy: Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.
- File Sharing/Podcasting: This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.
- Mashups: This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

Question 5

(a) As an IS auditor of a company, you want to use SCARF technique for collecting some information, which you want to utilize, for discharging some of your functions. Briefly describe the type of information that can be collected through the use of SCARF technique. (6 Marks)

(b) Describe the various benefits of Mobile Computing. (6 Marks)

(c) Feasibility Study is an important aspect of System Development Life Cycle (SDLC). Explain the dimensions, which are evaluated for this study. (4 Marks)

Answer

(a) The information that can be collected through the use of System Control Audit Review File (SCARF) technique is as follows:

- 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.

(b) The benefits of Mobile Computing are as follows:

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

(c) Feasibility Study is an important aspect of System Development Life Cycle (SDLC). The dimensions under which Feasibility Study of a system is evaluated are as follows:

- Technical Feasibility: Tries to get the answer of "Is the technology needed available?"

- Financial Feasibility: This checks "Is the solution viable financially?"
- Economic Feasibility: Deals with the question "Evaluation of the Return on Investment"
- Schedule/Time Feasibility: This handles "Can the system be delivered on time?"
- Resources: Deals with the concern on "Are human resources reluctant for the solution?"
- Operational Feasibility: Checks for the question "How will the solution work?"
- Behavioral Feasibility: Deals with "Is the solution going to bring any adverse effect on quality of work life?"
- Legal Feasibility: Answers the question "Is the solution valid in legal terms?"

Question 6

(a) The advent of computer has drastically transformed the mode of evidence collection by an auditor. Discuss the various issues involved in the performance of evidence collection and understanding the reliability of controls. (6 Marks)

(b) What are the steps to be taken by an IS auditor with respect to IT in the process of BCP/DRP audit? (6 Marks)

(c) Explain any four advantages of electronic door locks over bolting and combinational locks as a part of Physical Access Controls. (4 Marks)

Answer

(a) The advent of computer has drastically transformed the mode of evidence collection by an auditor. The issues involved in the performance of evidence collection and understanding the reliability of controls are as follows:

- 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.
- 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 printed 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 (journalised) 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 organisations 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.

(b) During a BCP/DRP Audit of Information Technology, IS auditor is expected to follow these steps:

- Determine if the plan reflects the current IT environment.
- Determine if the plan includes prioritization of critical applications and systems.
- Determine if the plan includes time requirements for recovery/availability of each critical system, and that they are reasonable.
- Does the disaster recovery/ business resumption plan include arrangements for emergency telecommunications?
- Is there plan for alternate means of data transmission if computer network is interrupted? Has the security of alternate methods been considered?
- Determine if a testing schedule exists and is adequate (at least annually). Verify the date of the last test. Determine if weakness identified in the last test were corrected.

(c) The following are the advantages of electronic door locks over bolting and combinational locks:

- Through the special internal code that is stored internally within the card; cards can be made to identify the correct individual.
- Individuals access needs can be restricted through the special internal code and sensor devices. Restrictions can be assigned to particular doors or to particular hours of the day.
- Degree of duplication is reduced.

- Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. If unauthorized entry is attempted silent or audible alarms can be automatically activated.
- An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also, parts of security. The card key becomes an important item to retrieve when an employee leaves the firm.

Question 7

Write short notes on any four of the following:

(a) Issues to be addressed by Information Security Policy.

(b) Any four major impacts of Technology on Internal Controls.

(c) Benefits of GEIT.

(d) Risk Management Strategies.

(e) Components of ERP. *(4 x 4 = 16 Marks)*

Answer

(a) The Information Security 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.

(b) The impact of Technology on Internal Controls is as follows:

- Competent and Trustworthy Personnel: Personnel should have proper skill and knowledge to discharge their duties. Substantial power is often vested in the persons responsible for the computer-based information systems developed, implemented, operated, and maintained within organizations.
- Segregation of Duties: In a computerized system, the auditor should be concerned with the segregation of duties within the IT department. As a basic control, segregation of duties prevents or detects errors or irregularities. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data, how it is processed and distribution and use of output.

- Authorization Procedures: In computer systems, authorization procedures often are embedded within a computer program. For example: In some on-line transaction systems, written evidence of individual data entry authorization, e.g. a supervisor's signature, may be replaced by computerized authorization controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).
- Adequate Documents and Records: In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions. Thus, no visible audit or management trail would be available to trace the transactions in a computerized system. However, if the controls over the protection and storage of documents, transaction details, and audit trails etc. are placed properly, it will not be a problem for auditor.
- Physical Control over Assets and Records: Physical control over access and records is critical in both manual systems and computer systems. Computerized financial systems have not changed the need to protect the data. A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located. This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster. The nature and types of control available have changed to address these new risks.
- Adequate Management Supervision: In computer system, data communication facilities can be used to enable employees to be closer to the customers they service. Thus supervision of employees might have to be carried out remotely. The Management's supervision and review helps to deter and detect both errors and fraud.
- Independent Checks on Performance: If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.
- Comparing Recorded Accountability with Assets: Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred. In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.
- Delegation of Authority and Responsibility: A clear line of authority and responsibility is an essential control in both manual and computer systems. In a computer system, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

(c) Benefits of Governance of Enterprise IT (GEIT) are 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.

(d) Risk management strategies are as below:

- 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.

(e) Components of Enterprise Resource Planning (ERP) are listed below:

(i) Software Component: The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligence.

(ii) Process Flow: It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model makes it easier to understand how ERP work.

(iii) Customer mindset: By implementing ERP system, the old ways for working which user understand and comfortable with have to be changed and may lead to users' resistance. In order to lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

(iv) Change Management: In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.