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

XYZ Ecom Ltd. is establishing an E-commerce platform to enable business to customer (B2C) process online. This platform will offer safe integrated supply process by e-linking suppliers, customers and bankers/payment gateways. The company proposes to keep the system 24 x7 working over internet. All concerned will be first registered with the databases of the company. All the data shall be stored across servers on internet based cloud environment in a secured manner.

Read the above carefully and answer the following:

(a) If the employees of the company are allowed to use personal devices such as laptop, smart-phones, tablets etc. to connect and access the data, what could be the security risks involved? Classify and elaborate such risks. (5 Marks)

(b) What are the advantages of using cloud computing environment? (5 Marks)

(c) In this company, what are your functions as an IS auditor? (5 Marks)

(d) List and explain the advantages of using continuous audit techniques for the proposed system. (5 Marks)

Answer

(a) The policy under which the employees of the company are allowed using Personal devices such as laptop, smart phones, tablets etc. to connect to the corporate network to access information and application is known as BYOD (Bring Your Own Device) policy. Under this, there will be certain amount of risk associated with the client's data, which can be classified into four areas given below:

- Network Risks: Under BYOD; when employees carry their own devices to workplace (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the company's network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need to be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.
- Device Risks: 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. Data lost from stolen or lost devices ranks as the top security threat.

- Application Risks: When a majority of employees' phones and smart devices are connected to the corporate network that are not protected by security software, probability of concurrent mobile vulnerabilities increase. Organizations become unclear in deciding that 'who is responsible for device security – the organization or the user'.
- Implementation Risks: Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

(b) Major advantages of Cloud Computing environment are given below:

- Cost Efficiency: Cloud computing is probably the most cost efficient method to use, maintain and upgrade. The cloud is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.
- Almost Unlimited Storage: Storing information in the cloud gives us almost unlimited storage capacity. Hence, one does not 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 automatic wherein no additional efforts are taken to customize and integrate the applications as per our preferences and 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: 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.

(c) Information System Auditor often is the assessor of business risk, as it relates to the use of IT, to management. The auditor can check the technicalities well enough to

understand the risk (not necessarily manage the technology) and make a sound assessment and present risk-oriented advice to management.

As an IS Auditor, we would review majorly the risks relating to IT systems and processes; some of which 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 lack of policies for use of Information and Communication Technology (ICT) resources; Internet usage policies; and Security practices etc.)
- IT-related frauds (including phishing; and hacking etc.)

(d) Some of the advantages of using continuous audit techniques for the proposed system are as under:

- Timely, Comprehensive and Detailed Auditing: Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed 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 Integrated Test Facilities (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 2

(a) 'MIS supports the managers at different levels to take decisions to fulfill the organizational goals.' Explain the major characteristics of MIS to achieve these goals.

(6 Marks)

(b) Explain the various plans that need to be designed for Business Continuity Management.

(6 Marks)

(c) 'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits. (4 Marks)

Answer

(a) 'Management Information System (MIS) supports the managers at different levels to take decisions to fulfill the organizational goals.' The major characteristics of MIS to achieve these goals are 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 as well.
- 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 their sufficient 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: MIS has an integrated approach as all the functional and operational information subsystems are 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 subsystems 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 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 period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- 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 by developing 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 management information system.

(b) There are various kinds of plans that need to be designed for Business Continuity Management (BCM) that 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. 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.
- 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 example, it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire. 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.
- Recovery Plan: The 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. Periodically, the recovery committee must review and practice executing their responsibilities so they are prepared in case a disaster occurs.
- Test Plan: The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plan 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.

(c) One of the well-known definitions of IT Governance is that "IT Governance is the system by which IT activities in a company or enterprise are directed and controlled to achieve business objectives with the ultimate objective of meeting stakeholder needs".

Some of the benefits of IT Governance are as follows:

- 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 3

(a) What is the role of IT in enterprises? Explain the different levels of managerial activity in an enterprise. (6 Marks)

(b) You have been associated with a system analysis team. Describe the important factors that you will consider while designing user input forms. (6 Marks)

(c) Briefly describe the key management practices provided by COBIT for ensuring IT compliances. (4 Marks)

Answer

(a) Role of IT in Enterprises is as under:

- In an increasingly digitized world, enterprises are using IT not merely for data processing but more for strategic and competitive advantage too. IT deployment has progressed from data processing to MIS to Decision Support Systems to online transactions/services.
- IT has not only automated the business processes but also transformed the way business processes are performed. IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

- The extent of technology deployment not only impacts the way internal controls are implemented in an enterprise but also provide better and innovative services from strategic perspective.
- An IT strategy aligned with business strategy ensures the value creation and facilitates benefit realization from the IT investments.
- Extensive organization restructuring or Business Process Re-Engineering may be facilitated through IT deployments.

The different levels of managerial activity in an enterprise are as under:

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

(b) The important factors that a system analysis team member will consider while designing user input forms are as follows:

- Content: This refers to the actual pieces of data to be gathered to produce the required output to be provided to users. The analyst is required to consider the types of data that are needed to be gathered to generate the desired user outputs. New documents for collecting such information may be designed.
- Timeliness: Timeliness refers to when users need outputs, which may be required on a regular, periodic basis - perhaps daily, weekly, monthly, at the of quarter or annually. Data needs to be inputted to computer in time because outputs cannot be produced until certain inputs are available. Hence, a plan must be established regarding when different types of inputs will enter the system.
- Format: Input format refers to the manner in which data are physically arranged. After the data contents and media requirements are determined, input formats are designed on the basis of few constraints like - the type and length of each data field as well as any other special characteristics (number decimal places etc.).
- Media: Input medium refers to the physical device used for input or storage. This includes the choice of input media and subsequently the devices on which to enter the data. Various user input alternatives may include display workstations, magnetic tapes, magnetic disks, key-boards, optical character recognition, pen-based

computers and voice input etc. A suitable medium may be selected depending on the application to be computerized.

- Form: Form refers to the way the information is inputted in the input form and the content is presented to users in various output forms - quantitative, non-quantitative, text, graphics, video and audio. Forms are pre-printed papers that require people to fill in responses in a standardized way. Forms elicit and capture information required by organizational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel.
- Volume: Input volume refers to the amount of data that has to be entered in the computer system at any one time. In some decision-support systems and many real-time processing systems, input volume is light. In batch-oriented transaction processing systems, input volume could be heavy which involves thousands of records that are handled by a centralized data entry department using key-to-tape or key-to-disk systems.

(c) COBIT 5 provides key management practices for ensuring IT compliance with external compliances as relevant to the enterprise. The practices are given as follows:

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

Question 4

(a) 'Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organisation'. What are the problems do you think that any organization can face with the result of computer crimes? (6 Marks)

(b) What are the factors influencing an organization towards controls and audit of computers? (6 Marks)

(c) As a member of IS Steering Committee, how do you classify the information for better integrity and security? (4 Marks)

Answer

(a) 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 given as follows:

- Financial Loss: Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.
- Legal Repercussions: An organization has to adhere to many laws while developing security policies and procedures. These laws protect both the perpetrator and organization from trial. The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures.
- Loss of Credibility or Competitive Edge: In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust. This credibility will be shattered resulting in loss of business and prestige if security violation occurs.
- Blackmail/Industrial Espionage: By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.
- Disclosure of Confidential, Sensitive or Embarrassing Information: These events can spoil the reputation of the organization. Legal or regulatory actions against the company may be also a result of disclosure.
- Sabotage: People, who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities. They do it because of their dislike towards the organization or for their intemperance.
- Spoofing: A spoofing attack involves forging one's source address. One machine is used to impersonate the other in spoofing technique. A penetrator makes the user think that s/he is interacting with the operating system. For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes the user login again.

(b) The factors influencing an organization towards controls and audit of 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.

(c) As a member of IS Steering Committee, the Information can be classified as under for better integrity and security:

- 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 etc., 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 be 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 be minimal.

Question 5

(a) What is meant by Information Security Policy? What are the components of a good security policy? (6 Marks)

(b) Describe the categories of tests that a programmer typically performs on a program unit. (6 Marks)

(c) As per IT (Amended) Act, 2008, describe the power to make the rules by Central Government in respect of Electronic Signature. (4 Marks)

Answer

(a) An Information Security Policy may be defined as a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide. In its basic form, an information security policy is a document that describes an organization's information security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business. An Information Security Policy is the essential foundation for an effective and comprehensive information security program. It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems.

Components of a good Security Policy

A good security policy should clearly state the following:

- Purpose and Scope of the Document and the intended audience;
- The Security Infrastructure;
- Security policy document maintenance and compliance requirements;
- Incident response mechanism and incident reporting;
- Security organization Structure;
- Inventory and Classification of assets;
- Description of technologies and computing structure;

- Physical and Environmental Security;
- Identity Management and access control;
- IT Operations management;
- IT Communications;
- System Development and Maintenance Controls;
- Business Continuity Planning;
- Legal Compliances; and
- Monitoring and Auditing Requirements.

(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.
- Performance Tests: 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.
- 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.

(c) Section 10 of IT (Amendment) Act, 2008, describes the Power to make rules by Central Government in respect of Electronic Signature. The Central Government may, for the purposes of this Act, by rules, prescribe

(a) the type of Electronic Signature;

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

(c) 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 6

(a) As an IS auditor, what are the environmental controls verified by you, while conducting physical inspections? (6 Marks)

(b) What is the need for an expert system in an organization? What are its benefits? (6 Marks)

(c) Describe the service strategy of ITIL, framework. (4 Marks)

Answer

(a) Audit of environmental controls requires the Information Systems '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 exits. 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) Major reasons for the need of Expert Systems are as follows:

- Expert labor is expensive and scarce. Knowledge workers/employees, who routinely work with data and information to carry out their day-to-day duties are not easy to find and keep and companies are often faced with a shortage of talent in key positions.

- Moreover, no matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.
- Both these limitations imposed by human information processing capability and the rushed pace at which business is conducted today put a practical limit on the quality of human decision making this putting a need for expert systems.

The key benefits of Expert Systems are given below:

- 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 it can be summoned almost as a real-life expert might be summoned.
- Expert Systems assist novices in thinking the way experienced professional 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.

(c) 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.

The components of service strategies are as follows:

- IT Service Generation
- Service Portfolio Management
- Financial Management
- Demand Management
- Business Relationship Management

Question 7

Write short notes on any four of the following:

(a) Objectives of IS audit.

(b) Metrics of risk management

(c) SDLC

(d) Third party site for backup and recovery.

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

Answer

(a) The major objectives of Information System Audit are as follows:

- Asset Safeguarding Objectives: The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
- Data Integrity Objectives: It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.
- System Effectiveness Objectives: Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
- System Efficiency Objectives: To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

(b) Metrics of Risk Management: Enterprises have to monitor the processes and practices of IT risk management by using specific metrics. 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.

(c) SDLC (System Development Life Cycle): The System Development Life Cycle 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. The SDLC is document driven, which means that a phase of the SDLC is not complete until the appropriate documentation or artifact is produced. Some of the advantages of this system are - Better planning and control by project managers; Compliance to prescribed standards ensuring better quality; Documentation that SDLC stresses on is an important measure of communication and control; and the phases that are important milestones and help the project manager and the user for review and signoff. The sequential phases of SDLC Cycle are as follows:

1. Preliminary investigation
2. Systems Requirements Analysis
3. Systems Design
4. Systems Acquisition

5. Systems Development
6. Systems Testing
7. Systems Implementation; and
8. Post Implementation Review and Maintenance

(d) If a third-party site is to be used for backup and 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; and
- What controls will be in place and working at the off-site facility?

(e) The components of ERP Model are as 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 Intelligent.

(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 need to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. 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.