1. (a) A System Development Methodology is characterized by the following:

- The project is divided into several identifiable processes, and each process has a starting point and an ending point. Each process comprises several activities, one or more deliverables and several management control points. The division of the project into these small, manageable steps facilitates both project planning and project control.

- Specific reports and other documentation, called Deliverables must be produced periodically during system development to make development personnel accountable for faithful execution of system development tasks.

- Users, managers, and auditors are required to participate in the project, which generally provide approvals, often called signoffs, at pre-established management control points. Signoffs signify approval of the development process and the system being developed.

- The system must be tested thoroughly prior to implementation to ensure that it meets users' needs as well as requisite functionalities.

- A training plan is developed for those who will operate and use the new system.

- Formal program change controls are established to preclude unauthorized changes to computer programs.

- A post-implementation review of all developed systems must be performed to assess the effectiveness and efficiency of the new system and of the development process.

(b) Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities. The six activities discussed below deal with system development controls in IT setup. These are given as follows:

- **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system’s authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.

- **User Specification Activities:** Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. However, it is most important that this document remains a statement of user needs. It should describe the user's view of the problem, not that of the systems professionals.
**Technical Design Activities:** The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long term success.

**Internal Auditor's Participation:** The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise. The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. Auditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.

**Program Testing:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors. Program testing is time-consuming, the principal task being the creation of meaningful test data. To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use. This will give the auditor a frame of reference for designing and evaluating future audit tests.

**User Test and Acceptance Procedures:** Just before implementation, the individual modules of the system must be tested as a unified whole. A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s). The formal test and acceptance of the system should consider being the most important control over the SDLC.

(c) Role of Information Technology (IT) in Enterprises are as follows:

- 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.

- The way in which business processes are performed/services rendered and how an organization is structured could be transformed through right deployment of IT. It is needless to emphasize that IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

- The extent of technology deployment also impacts the way internal controls are implemented in an enterprise.

Further, extensive organization restructuring or business process re-engineering may be facilitated through IT deployments. Implementing IT must consider not only implementation of IT controls from conformance perspective but also IT could be a key enabler for providing strategic and competitive advantage.
2. (a) Major limitations of Management Information Systems (MIS) are as follows:

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

(b) Major types of Information Systems (IS) Audits are as follows:

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

(ii) Information Processing Facilities: An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

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

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

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

(c) Major objectives of the Information Technology Act 2000 are given as follows:

- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as “electronic commerce” in place of paper-based methods of communication;
- To give legal recognition to Digital signatures for authentication of any information or matter, which requires authentication under any law;
To facilitate electronic filing of documents with Government departments;

To facilitate electronic storage of data;

To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;

To give legal recognition for keeping of books of accounts by banker’s in electronic form; and

To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker’s Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

3. **(a)** An audit or self-assessment of the enterprise’s BCM (Business Continuity Management) program should verify that:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprise’s BCM strategy;
- The enterprise’s BCM policy, strategies, framework and plans accurately reflect its priorities and requirements;
- The enterprise’ BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
- The enterprise’s BCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the enterprise;
- The enterprise’s BCM maintenance and exercising programs have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
- The enterprise has an ongoing program for BCM training and awareness;
- BCM procedures have been effectively communicated to relevant staff, and that those staff understand their roles and responsibilities; and
- Change control processes are in place and operate effectively.

**(b)** For the physical design of an Information System; the logical design is transformed into units, which in turn can be decomposed further into implementation units such as programs and modules. During physical design, the primary concern of the auditor is effectiveness and efficiency issues. The designers should follow some type of structured approach like CASE tools to access their relative performance via simulations when they undertake physical design. Some of the issues addressed here are type of hardware for client application and server application, Operating systems to be used, type of networking, processing – batch – online, real – time; frequency of input, output; and month-end cycles / periodical processing.

Some of the generic design principles being applied to develop the design of typical information systems include the following:

- There is a tendency to develop merely one design and consider it the final product. However, the recommended procedure is to design two or three alternatives and choose the best one on pre-specified criteria.
- The design should be based on the analysis.
• The software functions designed should be directly relevant to business activities.
• The design should follow standards laid down. For instance, the user interface should have consistent color scheme, menu structure, location of error message and the like.
• The design should be modular, with high cohesion and low coupling.

(c) 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.

4. (a) Despite the controls on place, there could be a possibility that a control might fail. When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls - A Disaster Recovery Plan (DRP) and Insurance.

• Disaster Recovery Plan (DRP): A comprehensive DRP comprise four parts – an Emergency Plan, a Backup Plan, a Recovery Plan and a Test Plan. The plan lays down the policies, guidelines, and procedures for all Information System personnel. BCP (Business Continuity Planning) Controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption. The controls include Critical Classification, alternative procedures, Back-up and Recovery, Systematic and Regular Testing and Training, Monitoring and Escalation Processes, Internal and External Organizational Responsibilities, Business Continuity Activation, Fall-back and Resumption plans, Risk Management Activities, Assessment of Single Points of Failure and Problem Management.

• Insurance: Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations. Policies usually can be obtained to cover the resources like – Equipment, Facilities, Storage Media, Valuable Papers and Records etc.

(b) The key management practices which are required for aligning IT strategy with enterprise strategy are highlighted here:

• 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 cooperation 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.

(c) 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 on the fleet. 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.

© The Institute of Chartered Accountants of India
• **Potential health hazards**: People who use mobile devices while driving is often distracted from driving are thus assumed more likely to be 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.

5. **(a)** When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Risk management strategy is explained and illustrated 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.

(b) **Financial Service Sector** – The financial services sector (banks, building societies, life insurance companies and short term insurers) manages large amounts of data and processes enormous numbers of transactions every day. Owing to application of IT, all the major financial institutions operate nationally and have wide networks of regional offices and associated electronic networks. The associated substantial client databases are handled via large central mainframe systems that characterize the industry. IT has changed the working style of financial services and makes them easier and simpler for customers also. Now-a-days most of the services are offered by the financial services on internet, which can be accessed from anywhere and anytime that makes it more convenient to the customers. It also reduces their cost in terms of office staff and office building. It has been observed that automated and IT enabled service sectors reduces cost effectively. Through the use of internet and mobile phones financial service sectors are in direct touch with their customers and with adequate databases it will be easier for service sectors to manage customer relationships. For example, through emails or SMS the customers can be made aware of launch of new policies; they can be informed on time the day of maturity of their policies etc.
In traditional banking system, the customer has to visit bank branch to deposit or withdraw money and get updated passbook from the respective counter. With the advancement of IT, the customer can do transactions by using internet banking, phone banking and the deposit or withdraw of money can also be done by using ATM (Automatic Teller Machine), internet or mobile banking. Banks also offers most of direct banking services free of charge to the customers. The customers can check the status of their accounts in different banks by using of direct banking. Retail banking in India has assured great importance recently with a number of retail banking products available to the consumer like real time account status, transfer of funds, bill payments and so on e.g. HDFC, SBI and ICICI are the banks in India that offer real time online transactions etc.

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

- Analysis of business processes and level of automation;
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business;
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture;
- Studying network diagrams to understand physical and logical network connectivity;
- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees and the government;
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems;
- Finally, studying Information Technology policies, standards, guidelines and procedures.

6. (a) Audit of Environmental Controls: 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 about 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) The activities involved in implementing Business Continuity in the Enterprise and Maintenance.
• Defining the scope and context;
• Defining roles and responsibilities;
• Engaging and involving all stakeholders;
• Testing of program on regular basis;
• Maintaining the currency and appropriateness of business continuity program;
• Reviewing, reworking and updating the business continuity capability, Risk Assessments (RA) and Business Impact Analysis (BIAs);
• Managing costs and benefits associated; and
• Convert policies and strategies into action.

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

7. (a) [Section 5] of Information Technology Act, 2000 is as follows:

[Section 5] Legal recognition of Electronic Signatures

Where any law requires that any information or matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

Explanation –

For the purposes of this section, “signed”, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand-written signature or any mark on any document and the expression “signature” shall be construed accordingly.

(b) Encryption: Encryption is the conversion of data into a secret code for storage in databases and transmission over networks. The sender uses an encryption algorithm and the original message called the clear text is converted into cipher text. This is decrypted at the receiving end. The encryption algorithm uses a key. The more bits in the key, the stronger are the encryption algorithms. Two general approaches are used for encryption viz. private key and public key encryption.
(c) **Economic Feasibility:** It includes an evaluation of all the incremental costs and benefits expected if the proposed system is implemented. After problems or opportunities are identified, the analysts must determine the scale of response needed to meet the user's requests for a new system as well as the approximate amount of time and money that will be required in the effort. The financial and economic questions raised by analysts during the preliminary investigation are for estimating the following:

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

After possible solution options are identified, an analyst should make a primary estimate of each solution's costs and benefits.

(d) **Security Management Controls**

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

(e) The different instances of SaaS are as follows:

- **Testing as a Service (TaaS):** This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.

- **API as a Service (APIaaS):** This allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.

- **Email as a Service (EaaS):** This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware.