1. (a) Factors that might have been considered while developing Input / Output Form Designs are as follows:

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Definition</th>
<th>Input Design</th>
<th>Output Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content</td>
<td>Refers to the actual pieces of data to be gathered to produce the required output to be provided to users.</td>
<td>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.</td>
<td>The contents of a weekly output report to a sales manager might consist of sales person’s name, sales calls made by each sales person during the week, and the amount of each product sold by each salesperson to each major client category.</td>
</tr>
<tr>
<td>Timeliness</td>
<td>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.</td>
<td>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.</td>
<td>A sales manager, may be requiring a weekly sales report. Other users, such as airline agents, require both real-time information and rapid response times in order to render better client service.</td>
</tr>
<tr>
<td>Format</td>
<td>Input format refers to the manner in which data are physically arranged. Output format refers to the arrangement referring to data output on a printed report or in a display screen.</td>
<td>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.).</td>
<td>Format of information reports for the users should be so devised that it assists in decision-making, identifying and solving problems, planning and initiating corrective action and searching.</td>
</tr>
<tr>
<td>Media</td>
<td>Input-output medium refers to the physical device used for input, storage or output.</td>
<td>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,</td>
<td>A variety of output media are available in the market these days which include paper, video display, microfilm, magnetic tape/disk and voice output.</td>
</tr>
<tr>
<td>Form</td>
<td>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. The form of the output should be decided keeping in view the requirements for the concerned user. For example - Information on distribution channels may be more understandable to the concerned manager if it is presented in the form of a map, with dots representing individual outlets for stores.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input Volume/Output Volume</td>
<td>Input volume refers to the amount of data that must be entered in the computer system at any one time. The amount of data output required at any one time is known as output volume. 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. It is better to use high-speed printer or a rapid-retrieval display unit, which are fast and frequently used output devices in case the volume is heavy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(b) Audit trails can be used to support security objectives in three ways:

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

- **Reconstructing Events**: Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign
responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

- **Personal Accountability**: Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behaviour. Individuals are likely to violate an organization’s security policy if they know that their actions are not recorded in an audit log.

(c) An audit or self-assessment of the enterprise’s BCM 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’s objectives);
- The enterprise’s 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.

2. (a) Some examples of Decision Support Systems (DSS) in Accounting are as follows:

- **Cost Accounting System**: The health care industry is well known for its cost complexity. Managing costs in this industry require controlling costs of supplies, expensive machinery, technology, and a variety of personnel. Cost accounting applications help health care enterprises calculate product costs for individual procedures or services. One health care organization, for example, combines a variety of DSS applications in productivity, cost accounting, case mix, and nursing staff scheduling to improve its management decision making.

- **Capital Budgeting System**: Companies require new tools to evaluate high-technology investment decisions. Decision makers need to supplement analytical techniques, such as net present value and internal rate of return, with decision support tools that consider some benefits of new technology not captured in strict financial analysis. One DSS designed to support decisions about investments in automated manufacturing technology is Auto Man, which allows decision makers to consider financial, non-financial, quantitative, and qualitative factors in their decision-making processes. Using this decision support system; accountants, managers and engineers identify and prioritize these factors. Then they can evaluate up to seven investment alternatives at once.

- **Budget Variance Analysis System**: Financial institutions rely heavily on their budgeting systems for controlling costs and evaluating managerial performance. One institution uses a computerized DSS to generate monthly variance reports for division comptrollers. The system allows these comptrollers to graph, view, analyze, and annotate budget variances, as well as
create additional one-and five-year budget projections using the forecasting tools provided in the system. The decision support system thus helps the comptrollers create and control budgets for the cost-center managers reporting to them.

- **General Decision Support System**: Some planning languages used in Decision Support Systems are general purpose and therefore can analyze many different types of problems. In a sense, these types of decision support systems are a decision-maker’s tools. The user needs to input data and answer questions about a specific problem domain to make use of this type of decision support system. An example is a program called Expert Choice which supports a variety of problems requiring decisions. The user works interactively with the computer to develop a hierarchical model of the decision problem. The DSS then asks the user to compare decision variables with each other.

(b) The three different types of audits that may be conducted during system development process are as follows:

- **Concurrent Audit**: Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.

- **Post-implementation Audit**: Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.

- **General Audit**: Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management’s assertions relating to the financial statements for systems effectiveness and efficiency.

(c) Once Business Continuity Plans (BCP) are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following:

- Defining the test purpose/approach;
- Identifying test teams;
- Structuring the test;
- Conducting the test;
- Analysing test results; and
- Modifying the plans as appropriate.

The approach taken to test the plans depends largely on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

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

- **Service Strategy:** This provides guidance on clarification and prioritization of service-provider investments in services;

- **Service Design:** This provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort;

- **Service Transition:** This relates to the delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than Business As Usual (BAU);

- **Service Operation:** This provides best practice for achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs), and

- **Continual Service Improvement:** This aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes.

(b) **Delineation of Scope:** The scope of a solution defines its typical boundaries. It should be clear and comprehensible to the user management stating the extent and 'what will be addressed by the solution and what will not'. Often, the scope becomes a contentious issue between development and user organizations. Hence, outlining the scope in the beginning is essential and proves quite handy. The typical scope determination may be performed on the following dimensions:

- **Functionality Requirements:** What functionalities will be delivered through the solution?

- **Data to be Processed:** What data is required to achieve these functionalities?

- **Control Requirements:** What are the control requirements for this application?

- **Performance Requirements:** What level of response time, execution time and throughput is required?

- **Constraints:** What are the conditions the input data must conform to? For example, what is the maximum number of characters that a name can have in a database?

- **Interfaces:** Is there any special hardware/software that the application must interface with? For example—Payroll application may have to capture from the attendance monitoring system that the company has already installed. Then the solution developer must understand the format of data, frequency mode of data transfer and other aspects of the software.

(c) **Threat:** Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat. A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. Threat has capability to attack on a system with intent to harm. It is often to start threat modeling with a list of known threats and vulnerabilities found in similar systems. Every system has a data, which is considered as a fuel to drive a system, data is nothing but assets. Assets and threats are closely correlated. A threat cannot exist without a target asset. Threats are typically prevented by applying some sort of protection to assets.

**Attack:** An attack is an attempt to gain unauthorized access to the system’s services or to compromise the system’s dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system. Basically, it is a set of actions designed to compromise CIA (Confidentiality, Integrity or Availability), or any other desired feature of an information system. Simply, it is the
act of trying to defeat Information Systems (IS) safeguards. The type of attack and its degree of success determines the consequence of the attack.

4. (a) **Community Cloud:** The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

Characteristics of Community Clouds are as follows:

- **Collaborative and Distributive Maintenance:** In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.
- **Partially Secure:** This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.
- **Cost Effective:** As the complete cloud is being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.

(b) The key governance practices required to implement Governance of Enterprise IT (GEIT) in enterprises are highlighted below:

- **Evaluate the Governance System:** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of governance of enterprise IT;
- **Direct the Governance System:** Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making; and
- **Monitor the Governance System:** Monitor the effectiveness and performance of the enterprise’s governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.

(c) The first Phase Pre-Planning Activities (Project Initiation) during the development of a Business Continuity Plan (BCP) is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to:

- refine the scope of the project and the associated work program;
- develop project schedules; and
- identify and address any issues that could have an impact on the delivery and the success of the project.

During this phase, a Steering Committee should be established. The committee should have the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. The Project Manager should work with the Steering Committee in finalizing the detailed work plan and developing interview schedules for conducting the Security Assessment and the Business Impact Analysis.

5. (a) Internal Control is comprised of five interrelated components:

- **Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is
manifested in management’s operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on. For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.

- **Risk Assessment:** This includes the elements that identify and analyse the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation. Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.

- **Control Activities:** This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

- **Information and Communication:** These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities. These are associated with control activities regarding information and communication systems of the entity that acts as one of the component of internal accounting system. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions. This includes the elements that ensure internal controls operate reliably over time. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

(b) Data Mining (DM) can be applied in database analysis and decision support i.e. market analysis and management by finding patterns that are helpful in target marketing, customer relation management, market basket analysis, cross selling, market segmentation, risk analysis, customer retention, improved underwriting, quality control, competitive analysis and fraud detection. Other applications of DM are:

- text mining,
- web analysis,
- customer profiling - it can list out what types of customers buy what products by using clustering or classification,
- identifying customer requirements - it can identify the most demanding and appropriate products for different customers, and can list the factors that will attract new customers by using prediction etc.,
- provide summary information i.e. various multidimensional summary reports and statistical summary information,
- finance planning and asset evaluation.

(c) **Inherent Risk:** Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, if there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor
concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same. Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.

6. (a) Information Systems Audit has been categorized into five types:

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

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

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

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

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

(b) In establishing and implementing the BCM system in the organization, managers from each function on site represent their areas of the operation. These people are also responsible for the ongoing operation and maintenance of the system within their area of responsibility.  

➢ Top management should appoint the Manager (BCM) role as being the role that is responsible for the BCM policy and its implementation. The Resource Planning Manager is supported by the Shift Leaders and Team Captains from each function, who are responsible for the ongoing implementation and maintenance of the BCM. The program should be communicated to all the stakeholders with appropriate training and testing. The enterprise may adopt any project management model for effective output.

➢ In implementation, the major activities that should be carried out include:

- 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) Based on the degree of human intervention, the Information System may be classified as Manual System or Automated System.

- In a **Manual System**, the activities like data collection, maintenance and final reporting are done by human.
In an Automated System; the activities like data collection, maintenance and final reporting are carried out by computer system or say machine itself.

7. (a) Section 7A of Information Technology Act, 2000

[Section 7A] Audit of Documents, etc. maintained in Electronic form

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

(b) Application Controls: These include the programmatic routines within the application program code. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, legal and regulatory requirements. Any function or activity that works to ensure the processing accuracy of the application can be considered an application control.

(c) The objectives of Systems Requirements Specification (SRS) are:

- To identify and consult the stake owners to determine their expectations and resolve their conflicts;
- To analyse requirements to detect and correct conflicts and determine priorities;
- To gather data or find facts using tools like - interviewing, research/document collection, questionnaires, observation;
- To verify that the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable;
- To model activities such as developing models to document Data Flow Diagrams, E-R Diagrams; and
- To document activities such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities.

(d) Detection Risk: Detection risk is the risk that the IT auditor’s substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.

(e) The two major components of Web 3.0 are as follows:

- **Semantic Web**: This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines can take contextual decisions on their own by finding, combining and acting upon relevant information on the web.

- **Web Services**: It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr to search for images.