

PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

QUESTIONS

Concepts of Governance and Management of Information Systems

1. List out the key functions of the IT Steering Committee.
2. 'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits.
3. Briefly describe the key management practices provided by COBIT 5 for ensuring IT compliances.

Information System Concepts

4. 'There are various constraints, which come in the way of operating a Management Information Systems (MIS)'. Explain any four such constraints in brief.
5. "A business manager should have adequate knowledge to operate Information Systems effectively". Elaborate this statement.
6. Discuss few examples of business applications of Expert Systems.

Protection of Information Systems

7. Discuss Application and Monitoring System Access Controls.
8. Discuss some Financial Controls Techniques.
9. Discuss about User Access Resource Management Controls.

Business Continuity Planning and Disaster Recovery Planning

10. Why do you think an organization needs to maintain a BCP Manual?
11. What does the methodology emphasize upon while developing a Business Continuity Plan (BCP)?
12. Explain the phase "Business Impact Assessment (BIA)" under Business Continuity plan methodology?

Acquisition, Development and Implementation of Information Systems

13. Discuss the roles of the following during SDLC (System Development Life Cycle).
 - (a) Steering Committee
 - (b) Database Administrator
 - (c) Project Leader
 - (d) Information Systems (IS) Auditor

14. Discuss the activities involved during the System Designing phase under SDLC (Systems Development Life Cycle).
15. Discuss the categories of tests that a programmer performs on a program unit during the phase System Testing under System Development Life Cycle (SDLC).

Auditing of Information Systems

16. As an auditor, what do you think are the disadvantages and limitations of using Continuous Audit Techniques?
17. Discuss the types of Managerial Controls and their scope, in brief.
18. Discuss Boundary Controls and their Audit Trails under Application Controls.

Information Technology Regulatory Issues

19. Identify and explain the Section of IT Act, 2000; that explains the situation(s) under which any computer or computer resources shall become liable to confiscation?
20. What do you understand by the term "IT Infrastructure Library (ITIL)"? Discuss its volumes in brief.

Emerging Technologies

21. Under Green Computing, discuss guidelines to conserve energy?
22. Discuss the limitations of Mobile Computing.
23. Discuss different instances of Infrastructure as a Service (IaaS) model in Cloud Computing.

Short Note Based Questions

24. Write short notes on following:
 - (a) COBIT Components
 - (b) Benefits of Office Automation Systems (OAS)
 - (c) Examples of Segregation of Duties (SoD)
 - (d) Features of Agile Manifesto
 - (e) Detection Risk

Questions based on Case Study

25. ABC is a company that provides tourism related services worldwide to its customers worldwide. Though its operations are all online, however, the current information infrastructure is not sufficient to sustain itself in the competitive environment. Thus, the management realizes that they need to develop a "Smart Tourism – IT infrastructure", which involves development of semantic based information system using Web 3.0 technologies, in cloud and mobile computing environment, for which a high-level IT

Steering Committee comprising IS Auditor as one of the members is appointed. The company also intends to develop a document for Disaster Recovery Plan after upgrading information infrastructure.

Read the above and answer the following questions:

- (a) What are the main objectives that an organization can achieve through Information Systems Auditing?
- (b) What are the various areas to be incorporated in the Disaster Recovery Planning Document? Indicate any ten such areas.
- (c) What do you mean by Web 3.0 Technology? Explain briefly two major components of Web 3.0 technology.

SUGGESTED ANSWERS/HINTS

1. The key functions of the IT Steering Committee would include the following:
 - To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
 - To establish size and scope of IT function and sets priorities within the scope;
 - To review and approve major IT deployment projects in all their stages;
 - To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
 - To review the status of IS plans and budgets and overall IT performance;
 - To review and approve standards, policies and procedures;
 - To make decisions on all key aspects of IT deployment and implementation;
 - To facilitate implementation of IT security within enterprise;
 - To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system between IT and its users; and
 - To report to the Board of Directors on IT activities on a regular basis.
2. **IT Governance:** IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.

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.
3. 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.
4. Major constraints which come in the way of operating a Management Information System are as follows:
- Non-availability of experts, who can diagnose the objectives of the organization and provide a desired direction for installing operating system. This problem may be overcome by grooming internal staff, which should be preceded by proper selection and training.
 - Experts usually face the problem of selecting the sub-system of MIS to be installed and operated upon. The criteria, which should guide the experts, depend upon the need and importance of a function for which MIS can be installed first.
 - Due to varied objectives of business concerns, the approach adopted by experts for designing and implementing MIS is a non-standardized one.

- Non-availability of cooperation from staff is a crucial problem, which should be handled tactfully. This task should be carried out by organizing lectures, showing films and also explaining to them the utility of the system. Besides this, some persons should also be involved in the development and implementation of the system.
5. To operate Information Systems (IS) effectively and efficiently, a business manager should have following knowledge about it:
- **Foundation Concepts** – It includes fundamental business, and managerial concepts e.g. ‘what are components of a system and their functions’, or ‘what competitive strategies are required’.
 - **Information Technologies (IT)** – It includes operation, development and management of hardware, software, data management, networks, and other technologies.
 - **Business Applications** – It includes major uses of IT in business steps i.e. processes, operations, decision making, and strategic/competitive advantage.
 - **Development Processes** – It comprise how end users and IS specialists develop and execute business/IT solutions to problems.
 - **Management Challenges** – It includes ‘how the function and IT resources are maintained’ and utilized to attain top performance and build the business strategies.
6. Some of the business applications of Expert Systems are as follows:
- **Accounting and Finance** - It provides tax advice and assistance, helping with credit-authorization decisions, selecting forecasting models, providing investment advice.
 - **Marketing** - It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centres, assisting with marketing timing decisions, determining discount policies.
 - **Manufacturing** - It helps in determining whether a process is running correctly, analysing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and facility layouts.
 - **Personnel** - It is useful in assessing applicant qualifications and assisting employees in filling out forms.
 - **General Business** - It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, and evaluating performance.
7. The Application and Monitoring System Access Controls are as follows:
- **Information access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user

can access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users. For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations.

- **Sensitive system isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment.

Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.

- **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.
 - **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.
 - **Clock synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.
8. Financial Controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. Some examples of financial control techniques are as below:
- **Authorization:** This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.
 - **Budgets:** These estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control. Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.
 - **Cancellation of documents:** This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a "paid" or "processed" stamp or punching a hole in the document.
 - **Dual control:** This entails having two people simultaneously access an asset. For example, the depositories of banks' 24-hour teller machines should be accessed and

emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two people: once access is achieved, only one person handles the asset. With teller-machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.

- **Input/ Output verification:** This entails comparing the information provided by a computer system to the input documents. This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.
 - **Safekeeping:** This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.
 - **Sequentially numbered documents:** These are working documents with pre-printed sequential numbers, which enables the detection of missing documents.
9. The User Access Resource Management Controls are as follows:
- **User Registration:** Information about every user is documented. The following questions are to be answered:
 - Why is the user granted the access?;
 - Has the data owner approved the access?; and
 - Has the user accepted the responsibility? etc. The de-registration process is also equally important.
 - **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities. For example, an operator at the order counter shall have direct access to order processing activity of the application system. S/he will be provided higher access privileges than others. However, misuse of such privileges could endanger the organization's information security. These privileges are to be minimal with respect to their job functions.
 - **User password management:** Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password.
 - **Review of user access rights:** A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.
10. An incident or disaster affecting critical business operations can strike at any time. Successful organizations need to maintain a comprehensive BCP Manual, which ensures process readiness, data and system availability to ensure business continuity. A BCP manual is a documented description of actions to be taken, resources to be used and

procedures to be followed before, during and after an event that severely disrupts all or part of the business operations.

- The BCP is expected to anticipate various types of incident or disaster scenarios and provide reasonable assurance to senior management of enterprise about the capability of the enterprise to recover from any unexpected incident or disaster affecting business operations and continue to provide services with minimal impact.
 - The BCP Manual is expected to specify the responsibilities of the BCM team, whose mission is to establish appropriate BCP procedures to ensure the continuity of enterprise's critical business functions. In the event of an incident or disaster affecting any of the functional areas, the BCM Team serves as liaising teams between the functional area(s) affected and other departments providing support services.
11. The methodology for developing a Business Continuity Plan (BCP) can be sub-divided into eight different phases; the extent of applicability of each phase must be tailored to the respective organization. The methodology emphasizes on the following:
- Providing management with a comprehensive understanding of the total efforts required to develop and maintain an effective recovery plan;
 - Obtaining commitment from appropriate management to support and participate in the effort;
 - Defining recovery requirements from the perspective of business functions;
 - Documenting the impact of an extended loss to operations and key business functions;
 - Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
 - Selecting business continuity teams that ensure the proper balance required for plan development;
 - Developing a business continuity plan that is understandable, easy to use and maintain; and
 - Defining how business continuity considerations must be integrated into ongoing business planning and system development processes in order that the plan remains viable over time.
12. The Phase "Business Impact Assessment (BIA)" under Business Continuity Plan methodology enables the project team to:
- identify critical systems, processes and functions;
 - assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities; and

- assess the “pain threshold,” that is, the length of time business units can survive without access to systems, services and facilities.

The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

13. (a) **Steering Committee:** It is a special high power committee of experts to accord approvals for go-ahead and implementations. Some of the functions of Steering Committee are as follows:
- To provide overall directions and ensures appropriate representation of affected parties;
 - To be responsible for all cost and timetables;
 - To conduct a regular review of progress of the project in the meetings of steering committee, which may involve co-ordination and advisory functions; and
 - To undertake corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.
- (b) **Database Administrator:** The data in a database environment has to be maintained by a specialist in database administration so as to support the application program. The DBA handles multiple projects; ensures the integrity and security of information stored in the database and also helps the application development team in database performance issues. Inclusion of new data elements has to be done only with the approval of the database administrator.
- (c) **Project Leader:** The project leader is dedicated to a project, who has to ensure its completion and fulfillment of objectives. S/he reviews the project status more frequently than a Project Manager and the entire project team reports to him/her.
- (d) **Information Systems (IS) Auditor:** As a member of the team, IS Auditor ensures that the application development also focuses on the control perspective. S/he should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software.
14. The System Designing phase under System Development Life Cycle (SDLC) include activities - Architectural Design; Design of the Data / Information Flow; Design of the Database; Design of the User-interface; Physical Design; and Design and acquisition of the hardware/system software platform', which are described briefly as follows:

- **Architectural Design:** Architectural design deals with the organization of applications in terms of hierarchy of modules and sub-modules. At this stage, we identify major modules; functions and scope of each module; interface features of each module; modules that each module can call directly or indirectly and Data received from / sent to / modified in other modules.
- **Design of Data/Information flow:** The design of the data and information flow is a major step in the conceptual design of the new system. In designing the data / information flow for the proposed system, the inputs that are required are - existing data / information flows, problems with the present system, and objective of the new system. All these have been identified in the analysis phase and documented in Software Requirements Specification (SRS).
- **Design of Database:** Design of the database involves determining its scope ranging from local to global structure. The scope is decided based on interdependence among organizational units. Conceptual Modeling, Data Modeling, Storage Structure Design and Physical Layout Design are the major activities involved in this activity.
- **User Interface Design:** It involves determining the ways in which users will interact with a system. The points that need to be considered while designing the user interface are - source documents to capture raw data, hard-copy output reports, screen layouts for dedicated source-document input, inquiry screens for database interrogation, graphic and color displays, and requirements for special input/output device.
- **Physical Design:** For the physical design, 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. 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.
- **System's Operating Platform:** In some cases, the new system requires an operating platform including hardware, network and system software not currently available in an organization. For example – a DSS might require high-quality graphics output not supported by the existing hardware and software. The new hardware/system software platform required to support the application system will then have to be designed for requisite provisions.
- **Internal Design Controls:** From internal control point of view, this phase is also an important phase as all internal controls are placed in system during this phase. The key control aspects at this stage include some concerns like - Whether all control aspects have been properly covered?; Whether controls put in place in system, appear in the documentation done at this stage?; and Whether a separate review of design document has been done by internal auditor?

15. 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.
16. Some disadvantages and limitations of the use of the continuous audit system are as follows:
- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
 - Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
 - Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
 - Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
 - Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.
17. The types of Managerial Controls and their scope are as follows:
- **Top Management and Information Systems Management Controls:** Discusses the top management's role in planning, organizing, leading and controlling the information

systems function. Also, provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.

- **System Development Management Controls:** Provides a contingency perspective on models of the information systems development process that auditors can use as a basis for evidence collection and evaluation.
 - **Programming Management Controls:** Discusses the major phases in the program life cycle and the important controls that should be exercised in each phase.
 - **Data Resource Management Controls:** Discusses the roles of the data administrator and database administrator and the controls that should be exercised in each phase.
 - **Quality Assurance Management Controls:** Discusses the major functions that quality assurance management should perform to ensure that the development, implementation, operation, and maintenance of information systems conform to quality standards.
 - **Security Management Controls:** Discusses the major functions performed by operations by security administrators to identify major threats to the IS functions and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level.
 - **Operations Management Controls:** Discusses the major functions performed by operations management to ensure the day-to-day operations of the IS function are well controlled.
18. **Boundary Controls:** These maintain the chronology of events that occur when a user attempts to gain access to and employ systems resources.
- Identity of the would-be user of the system;
 - Authentication information supplied;
 - Resources requested;
 - Action privileges requested;
 - Terminal Identifier;
 - Start and Finish Time;
 - Number of Sign-on attempts;
 - Resources provided/denied; and
- Accounting Audit Trail**
- Action privileges allowed/denied.

Operations Audit Trail

- Resource usage from log-on to log-out time.
 - Log of Resource consumption.
19. Section 76 under IT Act, 2000 explains about the situation under which any computer or computer resources that shall become liable to confiscation.

[Section 76] Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

20. 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. 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 volumes of ITIL are 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 relate 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.

21. Guidelines for Energy Conservation are as follows:

- Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;
- Develop a thin-client strategy wherein thin-clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;
- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;
- Power-up and power-down energy-intensive peripherals such as laser printers according to need;
- Employ alternative energy sources for computing workstations, servers, networks and data centers; and
- Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.

22. Limitations of Mobile Computing are as follows:

- **Insufficient Bandwidth:** Mobile Internet access is generally slower than direct cable connections using technologies such as GPRS and Enhanced Data for GSM and more recently 4G 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.
 - **Potential health hazards:** People who use mobile devices while driving are often distracted from driving and 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.
23. The different instances of Infrastructure as a Service (IaaS) model in Cloud Computing are as follows:
- **Network as a Service (NaaS):** NaaS, an instance of IaaS, provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on a per-per-use basis.
 - **Storage as a Service (STaaS):** STaaS, an instance of IaaS, provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. It is an ability given to the end users to store the data on the storage services provided by the service provider.
 - **Database as a Service (DBaaS):** This is also related to IaaS and provides users with seamless mechanisms to create, store, and access databases at a host site on demand. It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis. The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.
 - **Backend as a Service (BaaS):** It is a type of IaaS, that provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.
 - **Desktop as a Service (DTaaS):** It is an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. DTaaS is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades. The end-users are responsible for securing for managing their

own desktop images, applications, and security. These services are simple to deploy, highly secure and produce better experience on almost all devices.

24. (a) Components of COBIT are as follows:

- **Framework** - Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;
- **Process Descriptions** - A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.
- **Control Objectives** - Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
- **Management Guidelines** - Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes
- **Maturity Models** - Assess maturity and capability per process and helps to address gaps.

(b) Major benefits of Office Automation Systems (OAS) are as follows:

- Office Automation Systems improve communication within an organization and between enterprises.
- They reduce the cycle time between preparation of messages and receipt of messages at the recipients' end.
- They also reduce the costs of office communication both in terms of time spent by executives and cost of communication links.
- Office Automation Systems ensure accuracy of information and smooth flow of communication.

(c) Examples of Segregation of Duties (SoD) are as follows:

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

(d) Agile Manifesto is based on following 12 features:

- Customer satisfaction by rapid delivery of useful software;
- Welcome changing requirements, even late in development;
- Working software is delivered frequently (weeks rather than months);

- Working software is the principal measure of progress;
 - Sustainable development, able to maintain a constant pace;
 - Close, daily co-operation between business people and developers;
 - Face-to-face conversation is the best form of communication (co-location);
 - Projects are built around motivated individuals, who should be trusted;
 - Continuous attention to technical excellence and good design;
 - Simplicity;
 - Self-organizing teams; and
 - Regular adaptation to changing circumstances.
- (e) **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.
25. (a) Information Systems Auditing is the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both. This enables organizations to better achieve four major objectives that 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) The Disaster Recovery Planning document may include the following areas:
- The conditions for activating the plans, which describe the process to be followed before each plan, are activated.
 - Emergency procedures, which describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This should include arrangements for public relations management and for effective liaisoning with appropriate public authorities e.g. police, fire, services and local government.
 - Fall-back procedures, which describe the actions to be taken to move essential business activities or support services to alternate temporary locations, to bring business process back into operation in the required time-scale.
 - Resumption procedures, which describe the actions to be taken to return to normal business operations.
 - A maintenance schedule, which specifies "how and when the plan will be tested", and the process for maintaining the plan.
 - Awareness and education activities, which are designed to create an understanding of the business continuity, process and ensure that the business continues to be effective.
 - The responsibilities of individuals describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
 - Contingency plan document distribution list.
 - Detailed description of the purpose and scope of the plan.
 - Contingency plan testing and recovery procedure.
 - List of vendors doing business with the organization, their contact numbers and address for emergency purposes.
 - Checklist for inventory taking and updating the contingency plan on a regular basis.
 - List of phone numbers of employees in the event of an emergency.
 - Emergency phone list for fire, police, hardware, software, suppliers, customers, back-up location, etc.
 - Medical procedure to be followed in case of injury.
 - Back-up location contractual agreement, correspondences.
 - Insurance papers and claim forms.
 - Primary computer centre hardware, software, peripheral equipment and software configuration.

- Location of data and program files, data dictionary, documentation manuals, source and object codes and back-up media.
 - Alternate manual procedures to be followed such as preparation of invoices.
 - Names of employees trained for emergency situation, first aid and life saving techniques.
 - Details of airlines, hotels and transport arrangements.
- (c) **Web 3.0:** The term Web 3.0, also known as the Semantic Web, describes sites wherein the computers will be generated raw data on their own without direct user interaction. Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement and consolidation of dynamic web contents depending on the interest of the individual users. Web 3.0 technology uses the “Data Web” Technology, which features the data records that are publishable and reusable on the web through query-able formats. An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence.

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 in order to search for images.