FINAL – MAY 2018

PAPER 6: INFORMATION SYSTEMS CONTROL & AUDIT

Test Code:

Branch (MULTIPLE) Date:

(100 Marks)

Note: ***Question No.1 is compulsory. Candidates are required to answer any five questions from the remaining six questions.***

Question 1

(a) The policy under which the employees of the company are allowed using Personal devices such as laptop, smart phones, tablets etc. to connect to the corporate network to access information and application is known as BYOD (Bring Your Own Device) policy. **(1 mark)**

Under this, there will be certain amount of risk associated with the client's data, which can be classified into four areas given below:

Network Risks: Under BYOD; when employees carry their own devices to workplace (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the company's network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need to be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented. **(1 mark)**

Device Risks: A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threat. **(1 mark)**

Application Risks: When most employees' phones and smart devices are connected to the corporate network that are not protected by security software, probability of concurrent mobile vulnerabilities increase. Organizations become unclear in deciding that 'who is responsible for device security – the organization or the user'. **(1 mark)**

Implementation Risks: Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above-mentioned threats. **(1 mark)**

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

Cost Efficiency: Cloud computing is probably the most cost efficient method to use, maintain and upgrade. The cloud is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company. **(1 mark)**

<u>Almost Unlimited Storage</u>: Storing information in the cloud gives us almost unlimited storage capacity. Hence, one does not need to worry about running out of storage space or increasing the current storage space availability. **(1 mark)**

<u>Backup and Recovery</u>: Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage. **(1 mark)**

<u>Automatic Software Integration</u>: In the cloud, software integration is usually automatic wherein no additional efforts are taken to customize and integrate the applications as per our preferences and with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her enterprise. **(1 mark)**

<u>Easy Access to Information</u>: Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues. **(1/2 mark)**

<u>Quick Deployment</u>: Cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes. **(1/2 mark)**

(c) Information System Auditor often is the assessor of business risk, as it relates to the use of IT, to management. The auditor can check the technicalities well enough to understand the risk (not necessarily manage the technology) and make a sound assessment and present risk-oriented advice to management. **(2 mark)s**

As an IS Auditor, we would review majorly the risks relating to IT systems and processes; some of which are as follows:

- Inadequate information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.) **(1 mark)**

- Inefficient use of resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.) **(1 mark)**

- Ineffective IT strategies; policies and practices (including lack of policies for use of Information and Communication Technology (ICT) resources; Internet usage policies; and Security practices etc.) IT-related frauds (including phishing; and hacking etc.) **(1 mark)**

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

<u>Timely, Comprehensive and Detailed Auditing</u>: Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only. **(1 ½ mark)**

<u>Surprise test capability</u>: As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and

application system users being aware that evidence is being collected at that moment. This brings in the surprise test advantages. **(1 ½ mark)**

Information to system staff on meeting of objectives : Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency. **(1 mark)**

Training for new users: Using the Integrated Test Facilities (ITFs), new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports. **(1 mark)**

Question 2

a.

Corrective Controls: Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is a corrective control. Examples of Corrective Controls are given as follows: **(2 marks)**

- Contingency planning,
- Rerun procedures,
- Change input value to an application system, and
- Investigate budget variance and report violations.

The main characteristics of the corrective controls are given as follows: **(2 marks)**

- Minimizing the impact of the threat;
- Identifying the cause of the problem;
- Providing remedy to the problems discovered by detective controls;
- Getting feedback from preventive and detective controls;
- Correcting error arising from a problem; and
- Modifying processing systems to minimize future occurrences of incidents.

b. Audit trails can be used to support security objectives in the following 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. **(2 marks)**

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 tim e of a system failure can be used to assign responsibility and to avoid similar situations in 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. **(2 marks)**

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 behavior. Individuals are likely to violate an organization’s security policy if they know that their actions are not recorded in an audit log. **(2 marks)**

c. The SEBI norms for Auditor Selection are as follows:

Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the major Areas mentioned under SEBI’s Audit Terms of Reference (TOR). **(1 mark)**

The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium (ISC)^2. **(2 marks)**

The Auditor should have IT audit/governance frameworks and processes conform ing to industry leading practices like CoBIT. **(1 mark)**

The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. He should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited. **(1 mark)**

The Auditor may not have any cases pending against its previous auditees, which fall under SEBI’s jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task. **(1 mark)**

Question 3

a. TPS Components: The principal components of a TPS are given as follows:

Inputs – Source documents, such as customer orders, sales, slips, invoices, purchase orders, and employee time cards, are the physical evidence of inputs in to the Transaction Processing System. They serve several purposes like capturing data, facilitating operations by communicating data and authorizing another operation in the process, standardizing operations by indicating, which data require recording and what actions need to be taken and providing a permanent file for future analysis, if the documents are retained etc. Input of transactions may also be done in electronic form e.g. swiping and attendance card. **(1 mark)**

Processing – This involves the use of journals and registers to provide a permanent and chronological record of inputs. Journals are used to record financial accounting transactions, and registers are used to record other types of data not directly related to accounting. Some of the common journals are sales journal, purchase journal, cash receipts journal etc. **(1 mark)**

Storage – Ledgers and files provide storage of data on both manual and computerized systems. The general ledger, the accounts payable ledger, and the accounts receivable ledger are some of the records of a firm’s financial accounting transactions. **(1 mark)**

Outputs – Any document generated from the system is output. Some documents are both output and input. For example; a customer invoice is an output from the order -entry application system and also and input document to the customer. Financial reports summarize the results of transaction processing and express these results in accordance with the principles of financial reporting. **(1 mark)**

b. The Plan-Do-Check-Act (PDCA) cycle

ISO27001 prescribes 'How to manage information security through a system of information security management'. Such a management system consists of four phases that should be continuously implemented to minimize risks to the Confidentiality, Integrity and Availability (CIA) of information. **(2 marks)**

The PDCA cyclic process is explained below:

The Plan Phase (Establishing the ISMS) – This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls). **(1 mark)**
The Do Phase (Implementing and Working of ISMS) – This phase includes carrying out everything that was planned during the previous phase. **(1 mark)**

The Check Phase (Monitoring and Review of the ISMS) – The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives. **(1 mark)**

The Act Phase (Update and Improvement of the ISMS) – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase. **(1 mark)**

The cycle of these four phases never ends, and all the activities must be implemented cyclically to keep the ISMS effective. ISO/IEC 27001:2005 applies this to all the processes in ISMS.

c. Public Clouds: This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called provider clouds. Business models like SaaS (Software-as -a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services. **(2 marks)**

The Advantages of public cloud include the following: **(4 marks)**

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- There is no need for establishing infrastructure for setting up and maintaining the cloud.
- Strict SLAs are followed.
- There is no limit for the number of users.
- Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen. Further, privacy and organizational autonomy are not possible.

Question 4

a. If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover the following issues: **(1/2 mark each)**

- How soon the site will be made available after a disaster;
- The number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- The priority to be given to concurrent users of the site in the event of a common disaster ;
- The period during which the site can be used;
- The conditions under which the site can be used;
- The facilities and services the site provider agrees to make available;
- Procedures to ensure security of company's data from being accessed/damaged by other users of the facility; and
- What controls will be in place for working at the off-site facility.

b. Information classification does not follow any predefined rules. It is a conscious decision to assign a certain sensitivity level to information that is being created, amended, updated, stored, or transmitted. The sensitivity level depends upon the nature of business in an organization and the market influence. **(1 mark)**

The classification of information further determines the level of control and security requirements. Classification of information is essential to understand and differentiate between the value of an asset and its sensitivity and confidentiality. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level to ensure adequate security. **(1 mark)**

For many organizations, a very simple classification criterion is given as follows: **(4 marks)**

Top Secret: Highly sensitive internal information (e.g. pending mergers or acquisitions; investment strategies; plans or designs) that could seriously damage the organization if such information were lost or made public. Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level should be the highest possible.

Highly Confidential: Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations. Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants, patient's medical records and similar highly sensitive data. Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.

Proprietary: Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates. Such information is normally for proprietary use to authorized personnel only. Security at this level should be high.

Internal Use only: Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level should controlled but normal.

Public Documents: Information in the public domain; annual reports, press statements etc.; which has been approved for public use. Security at this level should minimal.

c. The advent of computer has drastically transformed the mode of evidence collection by an auditor. The issues involved in the performance of evidence collection and understanding the reliability of controls are as follows: **(1 mark each)**

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system.

- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.

- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.

- **Lack of availability of printed output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.

- **Audit evidence:** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.

- **Legal issues:** The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and who are the parties to the contract.

Question 5

a. **Risk Management Strategies:** 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. Various risk management strategies are explained as follows:

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. **(1 mark)**

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. **(1 mark)**

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. **(1 mark)**

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. **(1/2 mark)**

Turn back. Where the probability or impact of the risk is very low, then management may decide to ignore the risk. **(1/2 mark)**

b. There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows:

Unit Testing: Unit testing is a software verification and validation method in which a programmer tests if individual units of source code are fit for use. A unit is the smallest testable part of an application, which may be an individual program, function, procedure, etc. or may belong to a base/super class, abstract class or derived/child class. Unit tests are typically written and run by software developers to ensure that code meets its design and behaves as intended. The goal of unit testing is to isolate each component of the program and show that they are correct. A unit test provides a strict, written contract that the piece of code must satisfy. **(2 mark)**

There are five categories of tests that a programmer typically performs on a program unit. Such typical tests are described as follows: **(4 marks)**

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, 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, 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 can handle the situation.

Structural Tests: Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.

Parallel Tests: In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

c. There are various kinds of plans that need to be designed for Business Continuity Management (BCM) that include the following:

Emergency Plan: The Emergency plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g. major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked. **(2 marks)**

Back-up Plan: The Backup plan specifies the type of backup to be kept, frequency with which backup is to be undertaken, procedures for making backup, location of backup resources, site where these resources can be assembled and operations restarted, personnel who are responsible for gathering backup resources and restarting operations, priorities to be assigned to recovering the various systems, and a time frame for recovery of each system. For example, it might be difficult to specify; exactly how an organization's mainframe facility will be recovered in the event of a fire. The backup plan needs continuous updating as changes occur. For example, as personnel with key responsibilities in executing the plan leave the organization, the plan must be modified accordingly. **(2 marks)**

Recovery Plan: The Recovery plans set out procedures to restore full information system capabilities. Recovery plan should identify a recovery committee that will be responsible for working out the specifics of the recovery to be undertaken. The plan should specify the responsibilities of the committee and provide guidelines on priorities to be followed. The plan might also indicate which applications are to be recovered first. Periodically, the recovery committee must review and practice executing their responsibilities so they are prepared in case a disaster occurs. **(1 mark)**

Test Plan: The purpose of the test plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. **(1 mark)**

Question 6

a. The key management practices complying with COBIT 5 for assessing and evaluating the system of IT internal controls in an enterprise are given as follows:

Monitor Internal Controls: Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives. **(1 mark)**

Review Business Process Controls Effectiveness: Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively. It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing of controls,
continuous controls monitoring, independent assessments, command and control centers, and network operations centers. **(1 mark)**

Perform Control Self-assessments: Encourage management and process owners to take positive ownership of control improvement through a continuing program of self - assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts. **(1 mark)**

Identify and Report Control Deficiencies: Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders. **(1 mark)**

Ensure that assurance providers are independent and qualified: Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards. **(1/2 mark)**

Plan Assurance Initiatives: Plan assurance initiatives based on enterprise objectives and conformance objectives, assurance objectives and strategic priorities, inherent risk resource constraints, and sufficient knowledge of the enterprise. **(1/2 mark)**

Scope assurance initiatives: Define and agree with management on the scope of the assurance initiative, based on the assurance objectives. **(1/2 mark)**

Execute assurance initiatives: Execute the planned assurance initiative. Report on identified findings. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks. **(1/2 mark)**

b. The contracts and software licensing process consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming. **(1 mark)**
The following factors must be considered to validate a vendors' proposal at the time of software acquisition:

- The Performance capability of each proposed System in Relation to its Costs;
  The Costs and Benefits of each proposed system; **(1 mark)**

- The Maintainability of each proposed system; **(1 mark)**

- ♦ The Compatibility of each proposed system with Existing Systems; and Vendor Support. **(1 mark)**

c. **Information:** Technically, information means processed data that have been put into a meaningful and useful context. Data consists of facts, values or results, and information is the result of relation between data e.g. in a spread sheet student name, roll number and marks obtained in science and arts subjects represents data whereas the graph that shows the percentage of students, who acquired more than 80% in science subjects and 65% in arts subjects represents information. Information may be represented in the form of text, graph, pictures, voice, videos etc. **(1 mark)**

Mere collection of data is not information and mere collection of information is not knowledge. Information relates to description, definition, or perspective (what, who, when, where). Information is essential because it adds knowledge, helps in decision making, analyzing the future and acting in time. Information products produced by an information system can be represented by number of ways e.g. paper reports, visual displays, multimedia documents, electronic messages, graphics images, and audio responses. **(1 mark)**

Attributes of Information: Some of the important attributes of useful and effective information are given as follows:

Availability – It is a very important aspect of information. Information is useless if it is not available at the time of need.

Purpose/Objective – Information must have purposes/objective at the time it is transmitted to a person or machine, otherwise it is simple data. Depending upon the activities in an organization the Information communicated to people has a purpose. The basic objective of information is to inform, evaluate, persuade, and organize. This indeed helps in decision making, generating new concepts and ideas, identify and solve problems, planning, and controlling which are needed to direct human activity in business enterprises.

Mode and format – The modes of communicating information to humans should be in such a way that it can be easily understand by the people. The mode may be in the form of voice, text or a combination of these two. Format also plays an important role in communicating the idea. It should be designed in such a way that it assists in decision making, solving problems, initiating planning, controlling and searching. According to the type of information, different formats can be used e.g. diagrams, graphs, curves are best suited for representing statistical data. Format of information should be simple, relevant and should highlight important points but should not be too cluttered up.

Current/Updated – The information should be refreshed from time to time as it usually rots with time and usage. For example, the running score sheet of a cricket match available in Internet sites should be refreshed at fixed intervals of time so that the current score will be available. Similar is the case with broker who wants the latest information about the stock market.

Rate – The rate of transmission/reception of information may be represented by the ti me required to understand a situation. Useful information is the one which is transmitted at a rate which matches with the rate at which the recipient wants to receive. For example - information available from internet site should be available at a click of mouse, and one should not have to wait for it for an hour.

Frequency – The frequency with which information is transmitted or received affects its value. For example- weekly reports of sales show little change as compared to the quarterly reports and contribute less for assessing salesman capability.

Completeness and Adequacy – The information provided should be complete and adequate because only complete information can be used in policy making. For example - the position of student in a class can be found out only after having the information of the marks of all students and the total number of students in a class.

Reliability – It is a measure of failure or success of using information for decision - making. If information leads to correct decision on many occasions, we say the information is reliable.

Validity – It measures how close the information is to the purpose for which it asserts to serve. For example, the experience of employee does not support evaluating his performance.

Quality – It means the correctness of information. For example, the correct status of inventory is highly required.

Transparency – It is essential in decision and policy making. For example, giving only total amount of advances does not give true picture of utilization of funds for decision about future course of action; rather deposit-advance ratio may be more transparent information as it gives information relevant for decision making.

Value of information – It is defined as difference between the value of the change in decision behavior caused by the information and the cost of the information. In other words, given a set of possible decisions, a decision -maker may select one on basis of the information at hand. If new information causes a different decision to be made, the value of the new information is the difference in value between the outcome of the old decision and that of the new decision, less the cost of obtaining the information. **(4 marks)**

Question 7

Attempt any ***four*** *of the following*

7. (a) The key governance practices required to implement GEIT in enterprises are highlighted here:

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; **(1 ½ mark)**

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**(1 ½ mark)**

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. **(1 mark)**

(b) A good security policy should clearly state the following: **(1/2 mark each)**

♦ Purpose and Scope of the Document and the intended audience;

- The Security Infrastructure;
- Security policy document maintenance and compliance requirements;
- Incident response mechanism and incident reporting;
- Security organization Structure;
- Inventory and Classification of assets;
- Description of technologies and computing structure;
- Physical and Environmental Security;
- Identity Management and access control; IT Operations management;
- IT Communications;
- System Development and Maintenance Controls;
- Business Continuity Planning;
- Legal Compliances; and
- Monitoring and Auditing Requirements.

(c) *[Section 3]* **Authentication of Electronic Records**

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature. **(1 mark)**

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. **(1 mark)**

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generall y smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible

- to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record. **(1 mark)**

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair. **(1 mark)**

(d) Benefits of Mobile Computing are as follows:

It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts. **(1 mark)**

It enables mobile sales personnel to update work order status in real -time, facilitating excellent communication. **(1 mark)**

It facilitates access to corporate services and information at any time, from anywhere. **(1 mark)**

It provides remote access to the corporate Knowledgebase at the job location. **(1/2 mark)**

It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce. **(1/2 mark)**

(e) Strengths of Waterfall Model: The fundamental strength of the waterfall model has made it quite popular and handy among the fraternity. Major strengths are given as follows:

It is ideal for supporting less experienced project teams and project manage rs or project teams, whose composition fluctuates. **(1 mark)**

The orderly sequence of development steps and design reviews help to ensure the quality, reliability, adequacy and maintainability of the developed software. **(1 mark)**

Progress of system development is measurable. **(1 mark)**

It enables to conserve resources. **(1 mark)**

****