MOCK TEST PAPER – 2

FINAL (OLD) COURSE: GROUP – II

PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT

ANSWERS

MULTIPLE CHOICE QUESTIONS

1. **(b)** Business Governance

2. **(c)** Deterministic System

3. **(c)** Trojan Horse Attack

4. **(d)** Mirror backup

5. **(d)** Behavioral Feasibility

6. **(d)** Boundary Control

7. **(c)** IT Infrastructure Library (ITIL)

8. **(b)** Outsourced Private Cloud

9. **(b)** Evaluate, Direct and Monitor

10. **(d)** MIS is management oriented.

11. **(a)** Piggybacking

12. **(c)** To identify the critical business processes.

13. **(a)** It combines features of the prototyping model and waterfall model.

14. **(d)** No need of prior knowledge and experience of working with CAAT

15. **(b)** Punishment for sending offensive messages through communication service, etc.

16. **(c)** Yes, but require stringent SLAs

17. **(a)** Section 133 of Companies Act, 2013

18. **(c)** Tacit knowledge is articulated, and represented as spoken words, written material and compiled data

19. **(d)** Backup procedure

20. **(a)** Risk assessment, determination of recovery alternatives, recovery plan implementation, and recovery plan validation

21. **(b)** Project Manager

22. **(d)** Processing Controls

DESCRIPTIVE QUESTIONS

1. **(a)** The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and the how transparency of IT costs, benefits and risk is implemented. Some of the key metrics, which can be used for such evaluation, are:

- Percentage of IT enabled investments where benefit realization monitored through full economic life cycle;
- Percentage of IT services where expected benefits realized;

- Percentage of IT enabled investments where claimed benefits met or exceeded;
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits;
- Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

(b) **Information Security Policy** provides a definition of Information Security, its overall objective and the importance that applies to all users. Various types of information security policies are:

- **User Security Policies** – These include User Security Policy and Acceptable Usage Policy.
  - **User Security Policy –** This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners.
  - **Acceptable Usage Policy –** This sets out the policy for acceptable use of email, Internet services and other IT resources.
- **Organization Security Policies** – These include Organizational Information Security Policy, Network & System Security Policy and Information Classification Policy.
  - **Organizational Information Security Policy –** This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document.
  - **Network & System Security Policy –** This policy sets out detailed policy for system and network security and applies to IT department users.
  - **Information Classification Policy –** This policy sets out the policy for the classification of information.
- **Conditions of Connection –** This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers" systems.

(c) The number of management levels depends on the company size and organisation structure, but generally there are three such levels senior, middle and supervisory.

- Senior management is responsible for strategic planning and objectives, thus setting the course in the lines of business that the company will pursue.
- Middle management develops the tactical plans, activities and functions that accomplish the strategic objectives.
- Supervisory management oversees and controls the daily activities and functions of the tactical plan.

2. **(a)** Application security audit is being looked from the usage perspective. A layered approach is used based on the functions and approach of each layer. Layered approach is based on the activities being undertaken at various levels of management, namely supervisory, tactical and strategic. The approach is in line with management structure which follows top-down approach. For this, the IS auditors need to have a clear understanding of the following:

- Business process for which the application has been designed;
- The source of data input to and output from the application;
- The various interfaces of the application under audit with other applications;

- The various methods that may be used to login to application, other than normal user-id and passwords that are being used, including the design used for such controls;
- The roles, descriptions, user profiles and user groups that can be created in an application; and
- The policy of the organization for user access and supporting standards.

(b) During a BCP Audit, to determine if a disaster recovery/business resumption plan existed and was developed using a sound methodology, an IS Auditor would include the following elements:

- Identification and prioritization of the activities, which are essential to continue functioning.
- The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
- Operations managers and key employees participated in the development of the plan.
- The plan identifies the resources that will likely be needed for recovery and the location of their availability.
- The plan is simple and easily understood so that it will be effective when it is needed.
- The plan is realistic in its assumptions.

(c) **Batch Controls:** Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls called as Batch Controls can be exercises over the batch to prevent or detect errors or irregularities. Two types of batches occur:

- **Physical Controls:** These controls are groups of transactions that constitute a physical unit. For example – source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.
- **Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically contiguous. For example - different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.

3. **(a)** 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 also 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
- cross-sectional and time series analysis, and
- resource planning- it can summarize and compare the resources and spending.

(b) Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

- **Risk Assessment:** The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
- **Controls Assessment:** The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
- **Review of Documents:** It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

(c) The Reserve Bank of India (RBI) is India's central banking institution, which formulates the monetary policy with regard to the Indian rupee. The Bank was constituted for the need of following:

- To regulate the issue of banknotes,
- To maintain reserves with a view to securing monetary stability, and
- To operate the credit and currency system of the country to its advantage.

4. (a) Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. Overall, the risks associated with BYOD can be classified into four areas:

- **Network Risks:** It is normally exemplified and hidden in "Lack of Device Visibility". When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyse traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the 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 be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.
- **Device Risks:** It is normally exemplified and hidden in "Loss of Devices". 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 threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.
- **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that most employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that „who is responsible for device security – the organization or the user".
- **Implementation Risks:** It is normally exemplified and hidden in "Weak BYOD Policy". The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above-mentioned threats.

(b) A good Information Security policy should having following components:

- 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;
- Operations management;
- IT Communications;
- System Development and Maintenance Controls;
- Business Continuity Planning;
- Legal Compliances; and
- Monitoring and Auditing Requirements.

(c) The advantages of Business Continuity Management (BCM) are that the enterprise:

- is able to proactively assess the threat scenario and potential risks;
- has planned response to disruptions which can contain the damage and minimize the impact on the enterprise; and
- is able to demonstrate a response through a process of regular testing and trainings.

5. (a) Provisions of authentication of electronic records are given under Section 3 of Information Technology (Amendment) Act, 2008, which is given as follows:

[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.

(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.

Explanation -

For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally 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

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) 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.

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

(b) To review the Operations Management Controls implemented in an enterprise, auditors can use interviews, observations, and review of documentation to evaluate -

- the activities of documentation librarians;
- how well operations management undertakes the capacity planning ad performance monitoring function;
- the reliability of outsourcing vendor controls;
- whether operations management is monitoring compliance with the outsourcing contract; and
- whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

(c) **Program Documentation:** The writing of narrative procedures and instructions for people, who will use software is done throughout the program life cycle. Managers and users should carefully review both internal and external documentation to ensure that the software and system behave as the documentation indicates. If they do not, documentation should be revised. User documentation should also be reviewed for understandability i.e. the documentation should be prepared in such a way that the user can clearly understand the instructions.

6. **(a)** **(i)** **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 given 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.

(ii) **Project Manager:** A project manager is normally responsible for more than one project and liaisonsing with the client or the affected functions. S/he is responsible for delivery of the project deliverables within the time/budget and periodically reviews the progress of the project with the project leader and his/her team.

(iii) **Team Leader:** A project is divided into several manageable modules, and the development responsibility for each module is assigned to Module Leaders. For example, while developing a financial accounting application – Treasury, Accounts payable, Accounts receivable can be identified as separate modules and can be assigned to different module leaders. Module leaders are responsible for the delivery of tested modules within the stipulated time and cost.

(b) The seven Enablers of COBIT 5 are as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.

- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

(c) Section 65 of IT Act is related to "Tampering with Computer Source Documents".

[Section 65] Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.