FINAL – MAY 2018

INFORMATION SYSTEMS CONTROL AND AUDIT

Test Code –F85
Branch (Date : 04.03.2018)

(50 Marks)

Note: All questions are compulsory.

Question 1 (4*4 = 16 Marks)

Write short notes on:

(i) (all points are compulsory)

The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective Governance and Management framework that optimizes information and technology investment and use for the benefit of stakeholders.

a. Principle 1: Meeting Stakeholder Needs - COBIT 5 provides all the required processes and other enablers to support business value creation through the use of IT. An enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific; IT related goals and mapping these to specific processes and practices.
b. Principle 2: Covering the Enterprise End-to-End - COBIT 5 integrates governance of enterprise IT into enterprise governance. COBIT 5 covers all functions and processes within the enterprise and considers all IT related governance and management enablers to be enterprise -wide and end-to-end.
c. Principle 3: Applying a Single Integrated Framework - COBIT 5 is a single and integrated framework as it aligns with other latest relevant standard s and frameworks, thus allowing the enterprise to use COBIT 5 as the overarching governance and management framework integrator.
d. Principle 4: Enabling a Holistic Approach - COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT that require a holistic approach, taking into account several interacting components.
e. Principle 5: Separating Governance from Management - The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

(ii) Metrics of Risk Management (1 mark for each point)

Enterprises must monitor the processes and practices of IT risk management by using specific metrics. Some of the key metrics are as follows:

a. Percentage of critical business processes, IT services and IT -enabled business programs covered by risk assessment;
b. Number of significant IT related incidents that were not identified in risk Assessment;
c. Percentage of enterprise risk assessments including IT related risks; and
d. Frequency of updating the risk profile based on status of assessment of risks.

(iii) Green IT(1 mark for each point)

a. Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient, environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle.
b. It is largely taken as the study and practice of designing, manufacturing, using, and disposing of computers, servers, associated subsystems and peripheral devices efficiently and effectively with highly mitigated negative impact on the environment.

c. The goals of green computing are similar to green chemistry; reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste.
d. Many corporate IT departments have Green Computing initiatives to reduce the environmental impacts of their IT operations and things are evolving slowly but not as a revolutionary phenomenon.

(iv) Authentication of Electronic Records (Section 3) (1 mark for each point)

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

(b) 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

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

(c) Any person by the use of a public key of the subscriber can verify the electronic record.

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

Question 2 (6 Marks)

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. (1 mark)

Benefits of IT Governance (1/2 Mark for ach point)

a. Increased value delivered through enterprise IT;
b. Increased user satisfaction with IT services;
c. Improved agility in supporting business needs;
d. Better cost performance of IT;
e. Improved management and mitigation of IT-related business risk;
f. IT becoming an enabler for change rather than an inhibitor;
g. Improved transparency and understanding of IT's contribution to the business;
h. Improved compliance with relevant laws, regulations and policies; and More optimal utilization of IT resources.

Question 3 (6 Marks)

Role of IT in Enterprises is as under: (3 Marks)

a. In an increasingly digitized world, enterprises are using IT not merely for data processing but more for strategic and competitive advantage too. IT deployment has progressed from data processing to MIS to Decision Support Systems to online transactions/services.
b. IT has not only automated the business processes but also transformed the way business processes are performed. IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.
c. The extent of technology deployment not only impacts the way internal controls are implemented in an enterprise but also provide better and innovative services from strategic perspective.
d. An IT strategy aligned with business strategy ensures the value creation and facilitates benefit realization from the IT investments.
e. Extensive organization restructuring or Business Process Re -Engineering may be facilitated through IT deployments.

The different levels of managerial activity in an enterprise are as under: (3 Marks)

(i) Strategic Planning: Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources. It is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved.

(ii) Management Control: Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.

(iii) Operational Control: Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

Question 4 (5 Marks)

The set of skills that is generally expected of an IS auditor includes:

a. Sound knowledge of business operations, practices and compliance requirements; (1 mark)
b. Should possess the requisite professional technical qualification and certifications ; (1 mark)
c. A good understanding of information Risks and Controls; (1 mark)
d. Knowledge of IT strategies, policy and procedural controls; (1/2 mark)
e. Ability to understand technical and manual controls relating to business continuity; and(1/2 mark)
f. Good knowledge of Professional Standards and Best Practices of IT controls and security. (1/2 mark)
g. Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems. (1/2 mark)

Question 5 (6 Marks)

System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written on a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow -up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.(2 marks)

Auditors might use SCARF technique to collect the following types of information:

a. Application System Errors - SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.(1 mark)
b. Policy and Procedural Variances - Organizations must adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred. (1/2 mark)
c. System Exception - SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price(1/2 mark).
d. Statistical Sample - Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon. (1/2 mark)
e. Snapshots and Extended Records - Snapshots and extended records can be written into the SCARF file and printed when required. (1/2 mark)
f. Profiling Data - Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities. (1/2 mark)
g. Performance Measurement - Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system. (1/2 mark)

Question 6 (6 Marks)

(i) Yes, Mr. A is punishable for his activities under the Section 66F. (3 marks)

[Section 66F(1)(B)] Punishment for cyber terrorism

Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States,
public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be p unishable with imprisonment which may extend to imprisonment for life'.

Considering the facts provided in the case where Mr. A hacked into Defense Information System with an intention to steal classified information threatening the security and sovereignty of India, Mr. A is punishable for his activities.

(ii) Yes, Intermediary 'CyberNet' is liable under the Section 79. (3 marks)

[Section 79] Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him.

(2) The provisions of sub-section (1) shall apply if -

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government ma y prescribe in this behalf.

Thus, according to Section 79(2)(c); the Intermediary 'CyberNet' failed to observe due diligence in discharging his duties and also the other guidelines as prescribed by the Central Government. So, Intermediary 'CyberNet' is l iable.

Question 7 (5 Marks)

Major components that have been considered in Web 2.0 include the following:

- Communities: These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are several tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.

- Blogging: Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.

- Wikis: A Wiki is a set of co-related pages on a subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.

- Folksonomy: Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.

- File Sharing/Podcasting: This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.

- Mashups: This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps to find the exact information of a cell phone device from the internet, just by entering the cell number.

****