



INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)

Module E

(3 hours)

- Q.1 Secure Bank has recently consolidated its global IT operations by using a centralized, client-server based application. Demands of specialized operating skills to run the new setup are quite unique and cannot be met in-house. Management has therefore decided in principle, to outsource the centralized IT operations of the Bank to a third party service provider. Since the proposal is considered significant and risky, it needs to be approved by the Board of Directors. The Board has reviewed the proposal and has called a special meeting with the senior IT management of the Bank to evaluate the proposed outsourcing arrangement.

Required:

As part of the Board evaluation of proposed outsourcing arrangement; list at least twelve distinct questions which the Board should ask from the senior IT management, to satisfy itself about the above management proposal.

(12)

- Q.2 A lot of today's headlines tend to focus on identity theft and hackers breaking into corporate computer files to steal personal information. A newly formed firm of private consultants wants to chalk out a general plan to evaluate the risk management processes of its clients. You have been assigned to evaluate the process with reference to privacy of data and personal information.

Required:

Prepare a questionnaire which should ensure that all the relevant information about a client is obtained by the firm while carrying out the assigned task.

(10)

- Q.3 Smart Lease (SL) is a large-sized leasing company, primarily engaged in the leasing of automobiles and industrial equipments. Operations of the company are fully automated and are on custom-built IT applications. Over the last couple of years, the company has experienced a number of IT related security incidents such as sabotage, fraud, and theft of confidential or propriety information, both at head office and in branches. Management has analyzed these incidents and come to the conclusion that majority of these incidents were the work of insiders, i.e. employees of the company itself.

Required:

Suggest at least six IT security practices/controls which SL should establish to prevent or detect insiders' attacks on its IT resources. In each case explain the rationale behind your suggestion.

(12)

- Q.4 The new IT manager of SKY & Co. is skeptical about the effectiveness of the company's internal IT controls. He has identified that proper policies and procedures have not been documented. One of his foremost objectives is to restrict the use of illegal software and he has asked you to investigate and control such violations.

Required:

- (a) What audit procedures would you follow to identify software licensing violations? (03)
 (b) Suggest appropriate steps to prevent such violations. (04)

- Q.5 Data integrity is the heart of any application. Data integrity controls ensure the reliability of data and information for making management decisions. The higher the integrity of data, the greater shall be the credibility and reliability of the application system. As an information systems auditor reviewing an application, you have been asked to formulate an audit procedure to perform a data integrity controls review.

Required:

List the steps which would be included in the audit procedure for review of controls over data integrity. (06)

- Q.6 Advanced Industries Limited (AIL) had been using computerized system for its various information processing needs for the last many years. Recently, certain instances of control vulnerabilities have been observed. The management has come to the conclusion that the policies and procedures followed by it are mostly arbitrary and are not directed towards any specific control objectives.

Required:

List the key control objectives which any organization should aim to achieve while designing an information system. (05)

- Q.7 Mehrab Enterprises is a small company with a staff of 50 employees but only five of them use the accounting application. In the annual audit, lack of segregation of duties with regard to computer application usage was reported. As the head of accounts and IT sections you feel that the choices available with you are limited as further segregation was not possible unless more employees are hired. Therefore, you are determined to overcome this weakness through compensating controls.

Required:

Identify and explain the compensating controls which can mitigate the risk resulting from lack of segregation of duties. (06)

- Q.8 Electronic Data Interchange (EDI) is one of the first e-commerce applications in use between business partners for transmitting business transactions between organizations with different types of computer systems.

Required:

- (a) Identify the benefits associated with the adoption of EDI. (03)
 (b) Briefly describe five common risks associated with the adoption of EDI? Suggest relevant controls to address each type of risk. (10)

- Q.9 Buraq Air (BA) is a small sized airline with domestic operations only. As their IT auditor, you are reviewing the contingency planning of their information systems. During your review you observed that the disaster recovery plan (DRP) contains backup and standby arrangements only, while other areas are totally ignored. Moreover, the insurance policy relating to information systems, covers the loss of equipments only.

Required:

- (a) Identify the other areas which should also be covered in the DRP. (06)
 (b) Identify the main types of losses associated with information systems, which need to be insured. (03)

- Q.10 Computer Assisted Audit Techniques (CAAT's) are important tools for the IS auditor in gathering information from these environments. When systems have different hardware and software environments, different data structure, record formats, processing functions, etc., it is almost impossible for the auditors to collect evidence without a software tool to collect and analyze the records. CAAT's include various tools and techniques, one of which is Generalized Audit Software (GAS).

Required:

- (a) Which issues/areas an IS auditor should consider while selecting a CAAT to perform an audit procedure? (04)
- (b) Explain the functions which the GAS can perform. (04)

- Q.11 Connect Call Centre (CCC) has a country-wide setup of call centres. Mr. Khan has recently joined CCC as its Internal Auditor. Previously there was no formal internal audit department in the company; however, the internal audit function was performed by one of its business development managers. Mr. Khan has vast experience in quality assurance and internal audit. While reviewing IT acquisitions, he noted that though there was a structured acquisition policy in general, however the same was not being followed in case of IT procurements. All IT purchases, including high value acquisitions, are made by the IT department, after approval by Director Finance. However, the Director Finance, being a non-IT person, reviews the financial aspects only. As a result, in many cases the company was unable to make best use of its resources and the users remained unsatisfied. The IT Manager is aware of the inconsistencies but due to extreme pressure of work, he was more interested in getting things done. Consequently, poor negotiation and lack of good governance were evident from the prices and terms and conditions of various acquisitions. When Mr. Khan discussed his observations with Chief Executive Officer, he was advised to prepare a report based on his observations and recommendations.

Required:

On behalf of Mr. Khan, prepare a report for the board covering the following:

- (a) Brief introduction of the current situation as regards the IT acquisition process. (02)
- (b) Benefits that could be ensured by adopting a structured IT acquisition process. (04)
- (c) Brief explanation of core IT acquisition principles which CCC should follow. (06)

(THE END)