

**INSTITUTE OF COST AND MANAGEMENT ACCOUNTANTS  
OF PAKISTAN**

PROFESSIONAL-IV (NEW/EXISTING) EXAMINATION— SUMMER 2003

Friday, the 23rd May, 2003

79

**INFORMATION MANAGEMENT AND AUDITING/  
MANAGEMENT INFORMATION SYSTEMS-I**

*Time Allowed: 3 Hours*

*Maximum Marks : 70*

- (i) Attempt FIVE questions. All questions carry equal marks.
- (ii) Answer must be neat, relevant and brief.
- (iii) In marking paper, the examiners take into account clarity of exposition, logic of arguments, presentation, language and use of clear diagram/chart when necessary.
- (iv) Read the instructions printed on the top cover of answer script CAREFULLY before attempting the paper.
- (v) DO NOT write your Name, Reg. No. or Roll No., anywhere inside the answer script.
- (vi) There will be a computer based practical examination of 10 marks and presentation of a project of 20 marks which form a part of this paper.

**Special instructions for Question 1.**

Marks

- An overwritten reply will carry no mark.
- Use following format to answer this question.

Sr. No.	Your choice	Rationale (brief reason for your answer)
(i)		
so on		

Q. 1 Select the most appropriate answer from the choices given below:

14

- (i) If risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets" then risk has all of the following elements EXCEPT:
  - (a) Threats to and vulnerabilities of processes and/or assets.
  - (b) An impact on assets based on threats and vulnerabilities.
  - (c) Probabilities of the threats.
  - (d) Controls addressing the threats.
- (ii) Audit participation in the systems development process contributes to the value added goals of the organization. When such participation occurs, the IS Auditor should be aware of which of the following?
  - (a) An auditor's ability to perform an independent evaluation of the application after implementation will be impaired.
  - (b) An attitude and appearance of independence should be reflected in the auditor's conduct when conducting development reviews.
  - (c) As a control specialist, the auditor can provide significant value to the project team by making the final decision on specific controls.
  - (d) For ongoing evaluation capability, the auditor should ensure that computer audit software be implemented in all applications.

P.T.O.

- (iii) Which of the following department managers would be the BEST person to oversee the development of an information security policy?
- (a) Human Resources.
  - (b) Security Administration.
  - (c) Information Systems.
  - (d) Business Operations.
- (iv) When a complete separation of duties cannot be achieved in an online system environment, which of the following functions should be separated from the others?
- (a) Origination.
  - (b) Authorization.
  - (c) Recording.
  - (d) Correction.
- (v) Which of the following would an IS Auditor expect to find in a request for proposal (RFP), or an invitation to tender (ITT), for the provision of computer hardware?
- (a) Requirements for post implementation support and maintenance.
  - (b) Full details of the current computer hardware and software.
  - (c) The maximum budget allowed for the project.
  - (d) Corporate information, security policies, standards and procedures.
- (vi) Which of the following statements relating to packet switching networks is TRUE?
- (a) All packets for a given message travel the same route.
  - (b) Passwords can't be embedded within the packet.
  - (c) Packet lengths are variable and each packet contains the same amount of information.
  - (d) The cost charged for transmission is based on packet, not distance or route traveled.
- (vii) Which of the following BEST provides access control to payroll data being processed on a local server?
- (a) Logging of all access to personal information.
  - (b) Separate password for sensitive transactions.
  - (c) Software restricts access rules to authorized staff.
  - (d) System access restricted to business hours.
- (viii) Which of the following would be the MOST appropriate to ensure the confidentiality of transactions *via* the Internet?
- (a) Digital signature.
  - (b) Data Encryption Standard (DES).
  - (c) Virtual Private Network (VPN).
  - (d) Public Key Encryption.
- (ix) When implementing an application software package, which of the following presents the greatest risk?
- (a) Multiple software versions not controlled.
  - (b) Source program not synchronized with object code.
  - (c) Parameters not set correctly.
  - (d) Programming errors.

- (x) An IS Auditor should be involved in:
  - (a) Observing tests of the disaster recovery plan.
  - (b) Developing the disaster recovery plan.
  - (c) Maintaining the disaster recovery plan.
  - (d) Reviewing the disaster recovery requirements of supplier contracts.
- (xi) Which of the following would MOST likely ensure that a system development project meets business objectives?
  - (a) Maintenance of program change logs.
  - (b) Development of a project plan identifying all development activities.
  - (c) Release of application changes at specific times of the year.
  - (d) User involvement in system specification and acceptance.
- (xii) Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?
  - (a) Function point analysis.
  - (b) PERT chart.
  - (c) Rapid application development.
  - (d) Object-oriented system development.
- (xiii) Which of the following would be classified as a corrective control?
  - (a) Contingency planning.
  - (b) Procedures for transaction authorization.
  - (c) Use of access control software.
  - (d) Echo controls in telecommunications.
- (xiv) In a system that records all receivables for a company, the receivables are posted on a daily basis. Which of the following would ensure that receivables balances are unaltered between postings?
  - (a) Range Checks.
  - (b) Record Counts.
  - (c) Sequence checking.
  - (d) Run-to-run control totals.

- Q. 2 (a) With regard to system development, acquisitions and maintenance, describe any five of IS Auditor's tasks. Also explain how these tasks are performed? 10
- (b) Briefly describe at least two of the following System Development Tools and Productivity Aids: 4
- (i) Code Generators.
  - (ii) Computer Aided Software Engineering (CASE).
  - (iii) Fourth Generation Languages (4GLs).
  - (iv) Function Point Analysis.
- Q. 3 (a) Explain Continuous Audit Approach. 5
- (b) What are the various techniques of continuous audit approach? Compare and evaluate them. 9

P.T.O.

- Q. 4 A chain of super stores is expanding its outlets in Asia Pacific Region. Due to recent changes in technology (both software and hardware) they are planning to upgrade the software including the operating system software. A big question for the company in this latest system upgrade is of the compatibility. The vendor of the software has proved that the new software will reduce the operating cost of the company and will provide the expanded and enhanced services especially in inventory management to handle the huge volume of data.

**Required :**

- Discuss the above situation, as an IS auditor, with regard to: 14
- (a) The requirements.
  - (b) Technical issues.
  - (c) Alternatives.
  - (d) Cost/Benefit analysis.
  - (e) Views of personnel in IT department.
- Q. 5 Auditing Network Infrastructure Security is a challenging task. Explain the same with reference to:
- (a) Network Diagrams. 3
  - (b) Infrastructure. 3
  - (c) Logical security. 3
  - (d) Remote access. 3
  - (e) Development and change control. 2
- Q. 6
- (a) Who is database administrator (DBA)? 4
  - (b) Define the role of a DBA in IS department. 4
  - (c) What are the controls available to check DBA? 3
  - (d) How DBA is different from LAN administrator? 3
- Q. 7 When conducting a review of logical access exposures, why should an IS Auditor include the following in his review? Briefly explain each of them:
- (a) Application Systems Operation Manual. 2
  - (b) Policies, Procedures and Standards. 2
  - (c) Logical Access Security Policies. 2
  - (d) Formal Security Awareness and Training. 2
  - (e) Data Ownership. 2
  - (f) Data Owners. 2
  - (g) Data Custodians. 2

THE END