

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

PROFESSIONAL-IV EXAMINATION-SPRING (SUMMER), 2004

Thursday, the 27th May, 2004

751

INFORMATION MANAGEMENT AND AUDITING

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 Q. 1:

Marks

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

S No.	Your Choice	Rationale (Brief reason for your answer)
(i)		
(ii)		
and so on		

Q 1 Select the correct answer

14

- (i) An IS auditor, performing a review of an application's controls, discovers a weakness in system software, which could materially impact the application. The IS auditor should:
 - (a) disregard these control weaknesses as a system software review is beyond the scope of this review.
 - (b) conduct a detailed system software review and report the control weaknesses.
 - (c) include in the report a statement that the audit was limited to a review of the application's controls.
 - (d) review the system software controls as relevant and recommend a detailed system software review.

PTO

- (ii) The PRIMARY purpose of compliance tests is to verify whether:
 - (a) controls are implemented as prescribed.
 - (b) documentation is accurate and current.
 - (c) access to users is provided as specified.
 - (d) data validation procedures are provided.

- (iii) The MOST important responsibility of a data security officer in an organization is:
 - (a) recommending and monitoring data security policies.
 - (b) promoting security awareness within the organization.
 - (c) establishing procedures for IT security policies.
 - (d) administering physical and logical access controls.

- (iv) In a small organization, where segregation of duties is not practical, an employee performs the function of computer operator and application programmer. Which of the following controls should the IS auditor recommend FIRST?
 - (a) Automated logging of changes to development libraries.
 - (b) Additional staff to provide segregation of duties.
 - (c) Procedures that verify that only approved program changes are implemented.
 - (d) Access controls to prevent the operator from making program modifications.

- (v) When auditing a mainframe operating system, what would the IS auditor do to establish which control features are in operation?
 - (a) Examine the parameters used when the system was generated.
 - (b) Discuss system parameter options with the vendor.
 - (c) Evaluate the systems documentation and installation guide.
 - (d) Consult the systems programmers.

- (vi) Which of the following would allow a company to extend its enterprise's intranet across the Internet to its business partners?
 - (a) Client-Server.
 - (b) Virtual private network.
 - (c) Dial-Up access.
 - (d) Network service provider.

- (vii) The PRIMARY objective of a firewall is to protect:
 - (a) internal systems from exploitation by external threats.
 - (b) external systems from exploitation by internal threats.
 - (c) internal systems from exploitation by internal threats.
 - (d) itself and attached systems against being used to attack other systems.

- (viii) An IS auditor has just completed a review of an organization that has a mainframe and a client-server environment where all production data reside. Which of the following weaknesses would be considered the MOST serious?
- (a) The security officer also serves as the database administrator (DBA).
 - (b) Password controls are not administered over the client/server environment.
 - (c) There is no business continuity plan for the mainframe system's non-critical applications.
 - (d) Most LANs do not back up file server fixed disks regularly.
- (ix) An IS auditor discovers that an organization's business continuity plan provides for an alternate processing site that will accommodate fifty percent of the primary processing capability. Based on this, which of the following actions should the IS auditor take?
- (a) Do nothing, because generally, less than twenty-five percent of all processing is critical to an organization's survival and the backup capacity, therefore, is adequate.
 - (b) Identify applications that could be processed at the alternative site and develop manual procedures to backup other processing.
 - (c) Ensure that critical applications have been identified and that the alternate site could process all such applications.
 - (d) Recommend that the information processing facility arrange for an alternate processing site with the capacity to handle at least seventy-five percent of normal processing.
- (x) In an audit of a Business Continuity Plan (BCP) which of the following findings is of MOST concern?
- (a) There is no insurance for the addition of assets during the year.
 - (b) BCP manual is not updated on a regular basis.
 - (c) Testing of the backup of data has not been done regularly.
 - (d) Records for maintenance of access system have not been maintained.
- (xi) The PRIMARY purpose of undertaking a parallel run of a new system is to:
- (a) verify that the system provides required business functionality.
 - (b) validate the operation of the new system against its predecessor.
 - (c) resolve any errors in the program and file interfaces.
 - (d) verify that the system can process the production load.

- (xii) When auditing the requirements phase of a software acquisition, the IS auditor should. Marks
- (a) assess the feasibility of the project timetable.
 - (b) assess the vendor's proposed quality processes.
 - (c) ensure that the best software package is acquired.
 - (d) review the completeness of the specifications.
- (xiii) Which of the following procedures should be implemented to help ensure the completeness of inbound transactions via electronic data interchange (EDI)?
- (a) Segment counts built into the transaction set trailer.
 - (b) A log of the number of messages received, periodically verified with the transaction originator.
 - (c) An electronic audit trail for accountability and tracking.
 - (d) Matching acknowledgement transactions received to the log of EDI messages sent.
- (xiv) When conducting a review of business process re-engineering, an IS auditor found that a key preventive control had been removed. In this case, the IS auditor should.
- (a) inform management of the finding and determine if management is willing to accept the potential material risk of not having that preventing control.
 - (b) determine if a detective control has replaced the preventive control during the process and if so, not report the removal of the preventive control.
 - (c) recommend that this and all control procedures that existed before the process was reengineered, be included in the new process.
 - (d) develop a continuous audit approach to monitor the effects of the removal of the preventive control.
- Q 2 (a) What is the main objective of audit documentation? 4
- (b) What are the important considerations pertaining to audit documentation? Mention at least five. 5
- (c) List at least five audit documentations that should be maintained. 5
- Q 3 Management and auditors both take a lot of interest in policies and procedures.
- (a) What are organizational policies? Describe the role of management with regard to policies. 7
- (b) Describe the detailed procedures that are developed to implement organizational policies. What is the role of the IS Auditor when reviewing procedures? 7

- Q 4. IS Auditors often finds that output controls are amongst the most overlooked area in an organization. What do output controls ensure? Describe at least five (5) areas that an IS auditor should cover while reviewing the security of computer output. 14
- Q 5. Touring the Information Processing Facility (IPF) is useful while auditing physical access. Briefly state the following:
- (a) What does an auditor gain from this tour? 4
 - (b) What areas should be included in the tour? 4
 - (c) What documents should be looked to assist in the review? 6
- Q 6. Reciprocal agreement is one of the recovery alternatives for "Disaster Recovery" and "Business Continuity Planning". Briefly state the following:
- (a) The characteristics of reciprocal agreement. 6
 - (b) Advantages and disadvantages of reciprocal agreement. 8
- Q 7. The successful implementation of any system depends on correct integration of all the related components, and the planning for this should have been done at the beginning of the process. What are the factors that need to be considered for the implementation to happen effectively? 14

THE END