# IT/IS Auditing Question Paper – Set 2

Q.No.1. Which of the following is the major factor that affects the decision about performing an audit in an organization?

1. Purpose
2. Duration
3. Budget
4. Tools used

Q.No.2. Which of the following is the major factor affecting results of internal audits?

1. Performed by the internal employees
2. Lack of resources and finance
3. Internal employee relationships
4. Lack of professional capabilities.

Q.No.3 Which control classification attempts to repair the impact of a threat?

1. Preventive
2. Detective
3. Deterrent
4. Corrective

Q.No.4 Define Internal Controls?

1. Control Tools used to detect risks
2. Ensures proper functioning of processes within the company
3. Defines the efficient Audit procedures
4. Process in the Audit Planning

Q.No.5. Which is not an information security threat?

1. Computer assisted Fraud
2. Viruses
3. Poverty
4. Hacking

Q.No.6 What are the types of Internal Controls

1. Asses, Remove and Protect
2. Analyze, Design Process, Implement
3. Qualitative and Quantitative
4. Preventive, Detective, Reactive

Q.No.7 Which of the following is the best way for an auditor to determine the effectiveness of a security awareness and training program?

1. Interview a sample of employees
2. Review the security training program
3. Interview the training program developers
4. Review the security reminders to employees

Q.No.8 Reactive Internal Control is also called as

1. Preventive Control
2. Proactive Control
3. Corrective Control
4. Detection Control

Q.No.9 Logging all activities for later analysis is a

1. Corrective Control
2. Preventive Control
3. Detective Control
4. Proactive Control

Q.No.10 As an auditor you visit an organization for auditing and observe following things. Which of the following can be a threat for the organization?

1. You did not find any important documents lying on the desk of any employee
2. You observed that the entire campus is under video surveillance and regularly monitored
3. You observed that old paper records were dumped into the UPS room and the room was hot and a lot of dust was accumulated on the records.
4. You observed the visitor book just collects visitor name and mobile number and no ID proof of the visitor is checked

Q.No.11 Which of the following is the ideal Audit team reporting structure

1. CFO/CEO, IT Audit Team
2. CFO/CEO, IT Audit Committee, Director of Audits, Audit Manager, Audit Team
3. IT Audit Committee, Director of Audits, Audit Manager
4. Employees, Internal Audit team

Q.No.12 Which are the following are roles of System Administrator?

1. Create & Implement Access Control Policies
2. Employing security persons to guard resources
3. Enable and Archive logs
4. None of the above

Q.No. 13 --------------Internal Control does not prevent errors from occurring, but provides systematic way to detect and correct the situation

1. Proactive Control
2. Detective Control
3. Preventive Control
4. Corrective Control

Q.No.14 Which are the activities done during Audit Planning?

1. Field Work, Evaluation and Testing
2. Confirmation of planned actions, Audit Response verification
3. Internal Control questionnaire, Audit scopes, Objectives
4. Communication, Audit findings, Assesment results

Q.No. 15 Which of the following is not a Best Practice in securing a web server?

1. Up-to-date Web server
2. Run all possible services
3. Up-to-date OS
4. Enable Logging

Q.No. 16 A method of evaluating the security of a computer system or network by simulating an attack by a hacker is called as?

1. Incident Test
2. Security Test
3. Network Test
4. Penetration Test

Q.No. 17 As an auditor you require to check if the antivirus is installed on all the computers and is properly updated. There are almost 2000 computers in the organization. Which of the following method you will choose during auditing?

1. You will scan all 2000 computers to verify the requirement
2. You will scan only those computers which are critical to the organization
3. You will scan only those computers which are less critical and rarely used
4. You will select some critical systems and some rarely used systems to scan

Q.No. 18 Which of this data gathering technique is most important in auditing?

1. Review earlier audit reports
2. Interview employees based on audit questionnaire
3. Use various tools for system auditing
4. Review documents like policies, old audit reports etc.

Q.No. 19 Software Change controls, access controls, backup and recovery are examples of ------------------

1. Risk Management
2. Risks
3. Internal Controls
4. Assets of organization

Q.No.20 Identify the activities of Audit Assesment Phase.

1. Identify, Remove and Restore
2. Accept, Mitigate, Transfer
3. Fieldwork, Evaluation, Testing
4. Analyze, Resolve and Restore

Q.No. 21 Identify the outcome of Audit Planning Phase

1. Meeting, Scope, Objectives, Questionnaire, Plan and Checklist
2. Testing, Listing the audit findings, reporting
3. Testing, Evaluation and Eliminating the risks
4. Meeting, Scope and Testing.

Q.No. 22 Which of the following is not a port scanner

1. NMAP
2. SuperScan
3. Nessus
4. dig

Q.No. 23 Select the best option which describes Risk Management:

1. Identifying Risks
2. Treating Risks
3. Analyzing
4. All of the above

Q.No.24. Windows Logs include:

1. Application (program) events
2. Security-related events
3. System events.
4. All of the above

Q.No.25. Consider an Audit Issue - Developers have direct access to update production code. As an auditor what would be your recommendation

1. Ensure customer data is encrypted
2. Review the access rights
3. Allow the database management to the local administrator only.
4. Proper software change controls to be defined and implemented

Q.No. 26 If an Auditor wants to express an opinion, then he should have

1. Necessary qualification
2. Audit Evidence
3. Audit Recommendation
4. Audit questionnaire

Q.No. 27 Which of the following best defines Audit Sampling

1. Take samples for work
2. Select only few projects in an organization
3. Applying audit procedures to less 100% items inside a relevant population
4. Choose all possible samples and perform audit process

Q.No. 28 Consider an Audit Issue - The default umask on the server is set to 000. As an Auditor what would be your recommendation

1. Set umask to 000 on all critical servers
2. Remove umask on all critical servers
3. Raise a security issue on all critical servers
4. Set umask 027 on all critical servers

Q.No. 29 Buying an insurance for a company is a

1. Risk acceptance approach
2. Risk Transfer approach
3. Process of identifying the scape goat
4. Risk Mitigation approach

Q.No. 30 Identify the service that helps to setup firewall in Linux?

1. iptables
2. ypserv
3. ypbind
4. xinetd

Q.No.31 Which of the following is basic Risk Management Process?

1. Risk Analysis, Develop Plan, Take Action, Measure Results
2. Risk Analysis, Mitigate and Report
3. Risk identification, Resolving and Documenting
4. Risk Analysis, Develop Plan and Mitigate it

Q.No. 32 What is Event ID in Windows?

1. Tool to identify events
2. uniquely identifiable events that a Windows computer can encounterCompetitors
3. Security events have EventID
4. Critical events have EventID

Q.No. 33 When is the Audit Exit Meeting conducted?

1. During Assesment phase to tell the issues to the team
2. During Reporting phase
3. No exit meetings are conducted during any phase of Audit
4. During Planning phase

Q.No 34 Which of the following is true about the qualitative risk analysis?

1. It uses ratings such as High, Medium, and Low to tag the assets
2. It uses terms like Single Loss Expectancy, Safeguard Value etc.
3. It uses the cost of the assets
4. It uses mathematical formulas to calculate the loss due to a risk

Q.No 35 Which of the following is not true about the quantitative risk analysis method?

1. It uses the cost of the assets
2. It uses ratings such as High, Medium, and Low to tag the assets
3. It uses mathematical formulas to calculate the loss due to a risk
4. It uses terms like Single Loss Expectancy, Safeguard Value etc.

Q.No. 36 ISO 27001:2005 is a

1. Process
2. Procedure
3. Standard
4. Best Practice

Q.No. 37 Which of the following is the most important factor according to ISO 27001 for effective implementation of Information Security Management System (ISMS)?

1. Formation of a Risk analysis team
2. Active support from the top management
3. Formation of an internal audit team
4. Proper documentation of all ISMS activities

Q.No. 38 Which of the following phase cycle approach is described by ISO27001 for effective implementation of ISMS within an organization?

1. Plan-Do-Check-Act
2. Plan-Act-Check-Do
3. Act-Do-Check-Plan
4. Plan-Check-D0-Act

Q.No. 39 If Cost to replace a car is $10,000 and probability of car loss is 0.10, then calculate Risk?

1. Risk = $10,000 / 0.10
2. Risk = $10,000 \* 0.10
3. Risk = $10,000 + 0.10
4. Risk = $10,000 \* 0.10 + $10,000

Q.No. 40 Which of the following tool allows parsing and querying Logs using SQL statements?

1. Log Scanner on Windows
2. Log Parser on Windows
3. Cat /var/log/messages
4. Log server