**IT/IS Auditing Question Paper – Set 1**

**Q.No.1.** When an organization decides to insure some of its assets, what type of risk mitigation method they are adopting?

1. Risk Avoidance
2. Risk Reduction
3. Risk Transfer
4. Risk Elimination

Q.No.2. which of the following is true about Auditing (Definition)?

1. Helps in reducing the organization costs
2. Assesment of Organization’s internal policies, controls and process.
3. Addresses the Risk exposure within IT systems.
4. Defines better policies

.

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 of the following is the major step in the pre-audit preparation phase?

1. Review the procedures followed
2. Review organizations existing network diagram
3. Arrange a meeting with the senior management and take their inputs
4. Review the previous audit reports

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 most important phase of implementing information security?

1. Defining various security policies
2. Creating Service Level Agreements
3. Performing Risk analysis
4. Planning Audit activities

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 Which of the following is the right Audit Process?

1. Planning, Assesment, Follow-up and Reporting
2. Planning, Assesment, Reporting, Documenting
3. Planning, Design, Testing, Implementation
4. Planning, Assesment, Reporting, Follow-up

Q.No.11 Which type of control the security policy is?

1. Physical Preventive Control
2. Technical Preventive Control
3. Administrative Detective Control
4. Administrative Preventive Control

Q.No.12 How often should a business continuity plan be tested?

1. Whenever there are significant changes in the organization
2. Every Month
3. Half Yearly
4. Every three years

Q.No. 13 Choose the correct order:

1. Risk Quantification, Risk Management, Risk Treatment
2. Risk Analysis, Risk Quantification, Risk Treatment
3. Risk Management, Risk Quantification, Risk Analysis
4. Risk Analysis, Risk Management, Risk Quantification

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 a Security Audit Tool?

1. nmap
2. uname
3. cat /etc/passwd
4. /var/log/messages

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 Internal Information Security Auditor can \_\_\_\_\_\_\_\_\_.

1. Provide suggestion on implementing control
2. Configure the system to implement the control
3. Write code for implementing control
4. Take care of operating the control

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 Define Risk

1. The probability that a particular threat will exploit a particular vulnerability
2. Business is all about Risk and Reward
3. The probability that a particular vulnerability will exploit a particular threat
4. Risk is loss of money

Q.No.20 What are the three Risk based approaches?

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

Q.No. 21 An Indian Company opening a branch in Japan where earthquake is more often – This risk shall be

1. Not accepted
2. Accepted
3. Mitigated
4. Transferred

Q.No. 22 A HeartBleed OpenSSL bug in Payment Gateway services company – This risk should be

1. Accepted
2. Analyzed
3. Transfer to OpenSSL Development community
4. Mitigated

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. As an auditor you visit an organization for auditing and observe that the organization used USB pen drives to carry valuable data from one branch to another branch. Which following control you will suggest for the organization?

1. Encrypt the data on the pen drive with strong encryption software.
2. Management should use courier service for sending pen drives to branch offices
3. Use windows Encrypting File System.
4. Take some money as deposit from employee who carries the pen drive and if he loses the pen drive money will not be refunded to the employee

Q.No.25. During auditing you find that an organization is using real customer data for testing new application. Which of the following will be your recommendation on this issue?

1. perform data sanitization
2. **Ensure customer data is encrypted**
3. Review the access rights
4. Allow the database management to the local administrator only.

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 What does Audit Sampling lead to

1. Perfect Audit outcome
2. Better Audit recommendations
3. Audit Failure
4. Audit Sampling risk.

Q.No. 29 Which of the following is the major requirement for the OS auditing?

1. OS usually have a lot of security flaws
2. OS is the main component of the system and it hosts other applications
3. OS is the biggest software on the system
4. OS is frequently upgraded by the manufacturer.

Q.No. 30 Which of the following file holds the user password policy settings for a Linux operating system?

1. /etc/inittab
2. /etc/fstab
3. /etc/login.defs
4. /etc/security

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 are the various Threats to IT Systems?

1. Ex-employees
2. Social, Environment and Technical
3. Competitors
4. Security

Q.No. 33 Which of the following solution will allow you to immediately recover from a physical hard disk failure and access data?

1. Backup
2. RAID
3. Backup at remote site
4. A new spare hard disk

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 According ISO 27001:2005….

1. Documented procedure is required only for corrective action
2. Documented procedure is required only for preventive action
3. Documented procedure is required only for ISMS audits
4. Documented procedure is required for both corrective and preventive action.

Q.No. 38 Which of the following is the most important document that provides information about how ISO 27001 is implemented in that organization?

1. Start of Agreement
2. Source of Agreement
3. Source of Authority
4. Statement of Applicability

Q.No. 39 Which of the following command displays the high resource consuming processes on a Linux system?

1. top
2. ps aux
3. pgrep
4. kill

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