



COMPUTER SECURITY & AUDIT ASSURANCE (23CY705)

WORKSHEET

UNIT-III

CONDUCTING INFORMATION SYSTEM AUDIT

A. MCQs

1. The first phase of auditing is: [b]
 - a) Reporting
 - b) Planning
 - c) Testing
 - d) Monitoring
2. Risk assessment identifies: [b]
 - a) Opportunities
 - b) Threats
 - c) Employees
 - d) Assets
3. A vulnerability is: [b]
 - a) Strength
 - b) Weakness
 - c) Policy
 - d) Procedure
4. Penetration testing helps: [a]
 - a) Increase security
 - b) Reduce storage
 - c) Improve coding
 - d) Improve bandwidth
5. Interviews are used for: [a]
 - a) Information gathering
 - b) Risk elimination
 - c) Recovery planning
 - d) Encryption

B. Fill in the Blanks

1. Audit planning defines audit (Scope)
2. Risk assessment identifies (Threats)
3. Vulnerability scanning detects system (Weaknesses)
4. Security testing evaluates system (Security)
5. Banking audits focus on financial and IT (Controls)

C. Tutorial Problems

Problem 1

A bank launches an online banking platform.

Questions:

- Identify possible vulnerabilities.
- Suggest information gathering techniques.
- Recommend security testing methods.

Problem 2

An organization performs a risk assessment.

Questions:

- List risks associated with employee negligence.
- Propose mitigation strategies.