UNIT–III: Risk Conducting IS Audit

03

RISK ASSESSMENT

Modern Risk Auditing

Unit III focuses on the planning and execution phases of an Information System audit.

Key topics include risk assessment, vulnerability identification, security testing, and the specific needs of banking audits.

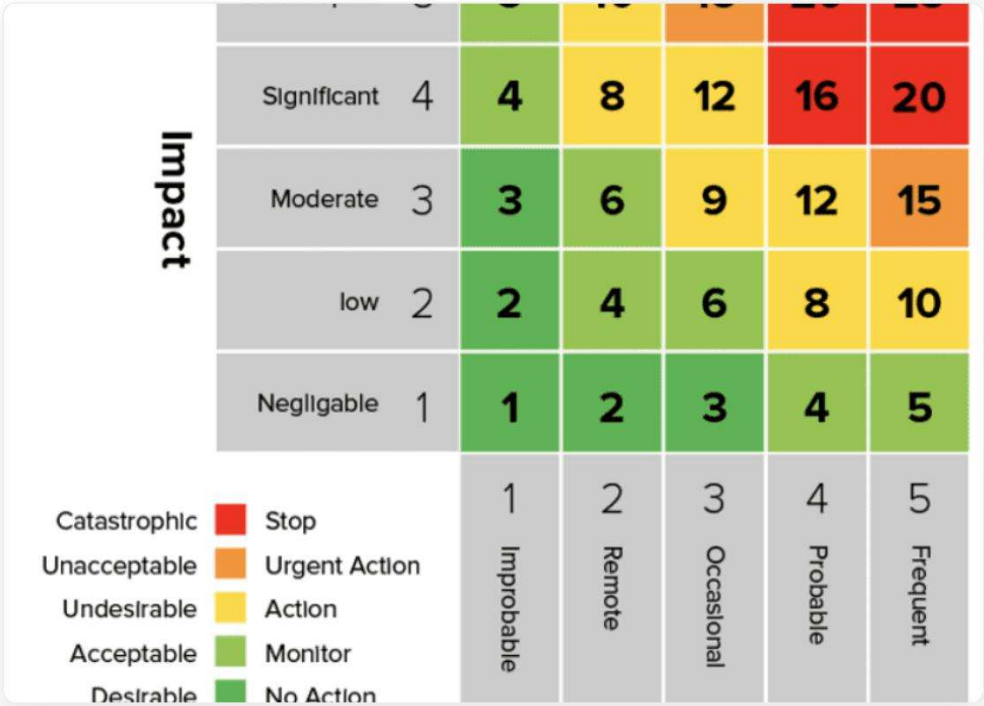
Steps in Audit Planning

Step Number	Activity	Objective
01	Define Objectives	Clarify what is being audited
02	Collect Information	Gather system documentation
03	Identify Risks	Pinpoint vulnerable areas
04	Prepare Schedule	Plan timeline and resource usage

The Risk Assessment Process

Risk assessment is the **heart of the audit**. It identifies threats and vulnerabilities that could impact assets.

- **Identify Assets:** List what needs protection.
- **Analyze Threats:** Evaluate likelihood of attack.
- **Estimate Impact:** Calculate financial/operational loss.



Audit Information Gathering

Interviews

Asking key personnel about workflows and security policies.

Observation

Physically watching how security controls are handled.

Questionnaires

Surveys to gather structured data from many staff members.

Common System Vulnerabilities

- **Weak Passwords:** Easy targets for brute force or dictionary attacks.
- **Unpatched Software:** Using versions with known security holes.
- **Malware:** Infections from malicious attachments or websites.

Prevention: Regular updates, strong firewalls, and comprehensive security training for staff.

System Security Testing Types

Penetration Testing

Authorized simulated attacks to find exploitable weaknesses.

Network Scanning

Identifying active hosts and services to verify network security posture.

Auditing Banks and ATMs

Banking audits are highly critical due to the direct involvement of financial assets.

- **Transaction Security:** Ensuring end-to-end encryption for every transfer.
- **ATM Security:** Checking physical anti-skimming and software integrity.
- **Customer Data:** Ensuring compliance with privacy laws regarding banking info.