IT Security Audit Checklist for Financial Institutions

> An **IT security audit checklist** for financial institutions ensures comprehensive evaluation of cybersecurity measures to protect sensitive financial data. It includes assessment of network security, access controls, and compliance with regulatory standards. Regular audits help identify vulnerabilities and strengthen the overall security posture of the organization.

1. Governance & Compliance

- Review policies and procedures related to IT security and data protection.
- Ensure compliance with financial regulations (e.g., GLBA, PCI DSS, SOX, GDPR if applicable).
- Verify maintenance of audit logs and incident response plans.
- Check for ongoing employee security awareness training.

2. Network Security

- Assess firewall configurations and rule sets for adequacy.
- Test intrusion detection/prevention systems (IDS/IPS).
- Ensure network segmentation for sensitive data environments.
- Scan for unpatched vulnerabilities and unauthorized devices.
- Evaluate secure remote access/VPN implementations.

3. Access Controls

- Audit user access rights and permissions based on the least privilege principle.
- Review multi-factor authentication (MFA) implementations for critical systems.
- Check for timely termination of access for former employees/contractors.
- Test password policies and enforcement mechanisms.

4. Data Security

- Verify encryption of sensitive data at rest and in transit.
- Review data backup and recovery procedures.
- Assess data loss prevention (DLP) controls.
- Ensure secure data destruction processes for end-of-life hardware/media.

5. Application Security

- Perform vulnerability scanning and penetration testing on critical applications.
- Check secure coding practices for in-house development.
- Update and patch software regularly to address known threats.
- Review third-party application risks and security controls.

6. Physical & Environmental Security

- Audit physical access controls to data centers and server rooms.
- Inspect environmental controls (fire suppression, climate control).

- Ensure secure disposal of printed documents containing sensitive information.

7. Incident Response & Monitoring

- Review incident detection, reporting, and escalation procedures.
- Test the incident response plan (tabletop exercises, real-world simulations).
- Check continuous security monitoring and alerting tools for effectiveness.

8. Vendor & Third-Party Management

- Assess third-party/vendor risk management policies.
- Review security requirements in vendor contracts and service level agreements (SLAs).
- Ensure regular security assessments of critical third parties.

9. Documentation & Reporting

- Maintain comprehensive records of all audit findings and remediation efforts.
- Report findings to management and relevant stakeholders.
- Track and verify closure of identified security issues.

10. Continuous Improvement

- Schedule regular reviews and updates to security policies and controls.
- Incorporate lessons learned from incidents and audits into policies and training programs.