Security Auditing Practices

- **Types of Audits:**
  - **Internal Audits:** Conducted by internal audit teams within the organization.
  - **External Audits:** Performed by independent third-party auditors.
  - **Compliance Audits:** Assess compliance with relevant laws and regulations (e.g., PCI DSS, HIPAA).
- **Audit Process:**
  - **Planning:** Define audit objectives, scope, and methodology.
  - **Execution:** Collect evidence, perform tests, and analyze findings.
  - **Reporting:** Document audit findings, including observations, recommendations, and corrective actions.
  - **Follow-up:** Monitor the implementation of corrective actions and ensure compliance.

Mock Internal Audit for TechServe (Example)

- **Objective:** To assess the effectiveness of the user access control policy.
- **Scope:** Review user account creation and modification procedures, access rights assigned to users, and the implementation of multi-factor authentication.
- **Findings:**
  - Some users had excessive privileges.
  - MFA was not enabled for all critical systems.
  - Password complexity requirements were not consistently enforced.
- **Recommendations:**
  - Implement the principle of least privilege.
  - Mandate MFA for all critical systems and administrative accounts.
  - Strengthen password complexity requirements and enforce them consistently.