7.9.2 Audit Facts

An *audit* is the activity of examining interpreting logs and other resources, settings, and relevant documentation to ensure that past actions or current configuration settings match the written security policy and that no unauthorized actions have taken place.

Be aware of the following auditing facts:

- Auditing usually involves reviewing an audit trail (also called a log or audit log).
- Audit logs should be periodically reviewed. The frequency will vary based on the the criticality of the system being monitored, but the logs must be reviewed on a scheduled basis by a knowledgeable member of the IT/Infosec team.
- Audit logs should be protected:
  - Use access controls that restrict access to and usage of the logs.
  - Use write once media to prevent tampering with audit logs.
  - Retain audit logs.
  - Notify the appropriate personnel if audit logs do not record the events they were set up to monitor.
  - Use the audit log of the system that has been attacked in the case of an incident.
- An *auditor* is a person who performs the following auditing activities:

Auditor	Description
Internal	An internal auditor is an employee within an organization that examines existing internal controls and maps the security structure for compliance with management's goals and statutes. Internal auditors are familiar with the organization and its goals, but might not have the skills of an external auditor; therefore, their findings might not be viewed as objective.
External	An external auditor works independently, either as a consultant or the employee of an auditing firm, to give an objective assessment of the security and controls structure of an organization. Though receiving an external audit can be very beneficial, it is important to be careful when allowing an external auditor to become familiar with the inner-workings of an organization. Make sure to examine the qualifications of the auditor and allow them sufficient time to learn about your organization.

An IT audit typically focuses on the computer systems and networks of an organization, but it may include aspects of physical security, as well. An IT audit includes:

- An assessment of computer systems and networks to determine the effectiveness of the technical and procedural controls.
- A risk evaluation, including:
  - Information security, such as maintaining current antivirus definition files
  - Inefficient use of corporate resources
  - Inefficient IT strategies, such as weak policies and procedures
  - IT-related fraud
- A user access and rights review, which determines whether privilege-granting processes are appropriate and whether computer use and escalation processes are in place and working.
- Privilege auditing, which checks user/group rights and privileges to identify cases of creeping privileges. It also aids in user/group administration.
- Usage auditing documents incidents for security violations and incident response. By reviewing user activity logs, compromised accounts can be identified, actions can be evaluated, and incidents can be replicated.
- Escalation auditing, which verifies the appropriate use of accounts and privileges. For example, administrators should be required to use normal user accounts for most activities. Administrators might circumvent these protections by granting additional privileges to their normal user accounts.

Security best practices require that audit logs be reviewed regularly. When determining what to review and how frequently, balance the organization's security needs with the amount of data to review.

Two important government and industry audits are:

Audit	Description
SOX	A Sarbanes-Oxley (SOX) audit is a government audit by the SEC that relates to internal controls and focuses on IT security, access controls, data backup, change management, and physical security.
PCI	Personal Card Industry (PCI) compliance audits relate to the use of credit cards. These audits are regulated and enforced by the major credit card companies. Failing PCI audits can result in heavy fines or losing the ability to accept credit cards as a method of payment. These audits focus on how credit card data is used, stored or not stored, and the physical security surrounding employees who receive credit card payments.