14.1.2 Audit Facts

An *audit* is the process of examining logs and relevant resources, settings, and documentation to ensure that past actions and current configuration settings match the written security policy and that no unauthorized actions have taken place. It also examines adherence to compliance requirements, laws, and regulations.

This lesson covers the following topics:

- Internal audits
- External audits
- IT Security audits
- Financial audits

Internal Audits

An internal auditor is an employee within an organization who examines existing internal controls and maps the security structure for compliance with statutes and management's goals. Internal auditors are familiar with the organization and its goals, but might not have the skills of an external auditor. Therefore, their findings might be viewed as:

- Not as formal
- Not objective
  - Internal audits focus on improvement and don't negatively affect customer contracts.
  - Internal audits by nature tend to be nonobjective and consequently may not be as rigorous.

External Audit

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. An external auditor can also be a government employee if a company works on government contracts. 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 the auditor sufficient time to learn about your organization. An external audit:

- Is a very formal and structured process
- Strictly adheres to compliance obligations
  - It is important to fully understand exactly what the purview of the audit is and require the auditor to follow it.
  - You should have a contact and communication strategy in place prior to the audit to help to keep the auditor from job creep.

IT Security Audits

An IT security audit typically focuses on the security posture of a company. The audit is comprised of the examination of network security, implementation of the principle of least privilege (PoLP), adherence to relevant standards as well as written business continuity and disaster recovery plans. It normally includes physical security, as well. Two components of an IT security audit are:

Component	Description

Risk evaluation or assessment	The risk assessment includes evaluation of: - Defense in depth. - Proper governance policies. - Current redundancy plans. - Proper use of corporate technology resources. - Company and IT security strategies, policies and procedures. - IT related fraud.
User access and rights review	Privilege auditing examines: - Use of roles and other security groups to grant access and privileges to network users. - Implementation of PoLP. - Implementation of policies that prevent privilege creep. - Documentation of security violations and incident response. - Review of user activity logs to identify compromised accounts, evaluate actions, and replicate incidents. - Use of escalation auditing to verify 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.

Financial Audits

This table shows two important financial audits that you will likely face. The first is a Sarbanes-Oxley (SOX) compliance review. SOX is a federal law. The second is a Personal Card Industry (PCI) Data Security Standard (DSS) audit. PCI DSS is a compliance requirement established by the major credit card issuers.

SOX	A Sarbanes-Oxley 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 DSS	Payment Card Industry Data Security Standard 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.

The above listed audit examples are not all inclusive but an introduction into the world of network security and data auditing. Contracts and SLAs are a determining factor in frequency and type of audits required.