2.4.3 Assessment Type Facts

A organization's purpose for completing a penetration test will dictate how the test will be carried out. Depending on the penetration test's goals, the ethical hacker may have specific rules and regulations that need to be observed. There are scenarios that will result in special considerations being made.

This lesson covers the following topics:

- Goal-based penetration test
- Objective-based penetration test
- Compliance-based penetration test
- Special considerations

Goal-Based Penetration Test

A goal-based penetration test will focus on the end results. The goals must be specific and well-defined before the test can begin. The penetration tester will utilize a wide range of skills and methods to carry out the test and meet the goals. When you determine the goals of the exam, you should use S.M.A.R.T. goals.

- S – Specific
- M – Measurable
- A – Attainable
- R – Relevant
- T – Timely

Objective-Based Penetration Test

An objective-based test focuses on the overall security of the organization and its data security. When people think of a penetration test, this is often what they think of. The scope of work and rules of engagement documents specify what is to be tested.

Compliance-Based Penetration Test

Ensuring that the organization is in compliance with federal laws and regulations is a major purpose for performing a penetration test. Some of the main laws and regulations include the following:

Regulation	Description
Payment Card Industry Data Security Standards (PCI-DSS)	Defines the security standards for any organization that handles cardholder information for debit cards, credit cards, prepaid cards, and other types of payment cards.
Health Insurance Portability and Accountability Act (HIPAA)	A set of standards that ensures a person's health information is kept safe and only shared with the patient and medical professionals that need it.
ISO/IEC 27001	Defines the processes and requirements for an organization’s information security management systems.
Sarbanes Oxley Act (SOX)	A law enacted in 2002 with the goal of implementing accounting and disclosure requirements that would increase transparency in corporate governance and financial reporting and formalizing a system of internal checks and balances.
Digital Millennium Copyright Act (DMCA)	Enacted in 1998, this law is designed to protect copyrighted works.
Federal Information Security Management Act (FISMA)	Defines how federal government data, operations, and assets are handled.

Special Considerations

There are a few scenarios where extra or special considerations need to be taken into account, such as mergers and establishing supply chains. During a merger, a penetration test may be performed to assess physical security, data security, company culture, or other facets of an organization to determine if there are any shortcomings that may hinder or cancel the merger. When establishing a supply chain, a penetration test needs to be performed to determine if there are any security issues or violations that could affect everyone involved. The organizations need to ensure that their systems can talk to each other and their security measures align. For these tests, companies may employ red teams and blue teams. They may also utilize purple team members.
