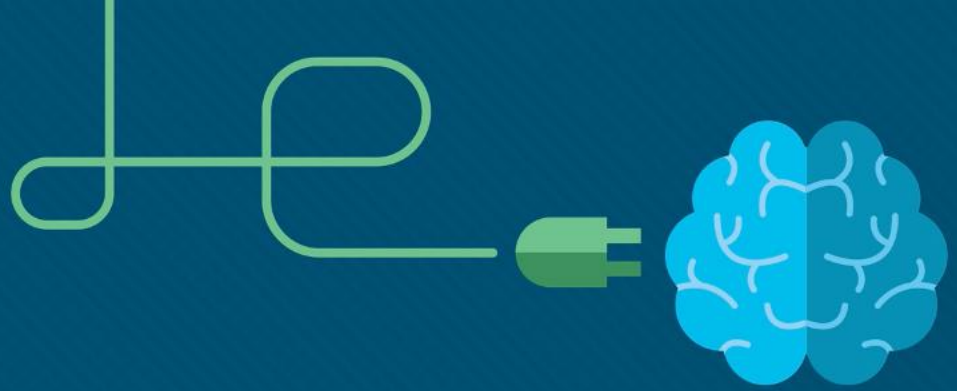


Module 2: Planning and Scoping a Penetration Testing Assessment

Ethical Hacker

Module Objectives

Module Title: Planning and Scoping a Penetration Testing Assessment

Module Objective: Create penetration testing preliminary documents.

Topic Title	Topic Objective
Comparing and Contrasting governance, Risk, and Compliance Concepts	Explain how governance, risk, compliance, and environmental factors in planning penetration testing.
Explain the Importance of Scoping and Organizational or Customer Requirements	Create a penetration test scope and plan document that addresses organizational requirements for penetration testing services.
Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity	Create your personal code of conduct to provide professionalism and integrity in your ethical hacking practice.

2.1 Comparing and Contrasting Governance, Risk, and Compliance Concepts

Overview

- One of the most important phases (if not the most important) of any penetration testing engagement is the planning and preparation phase.
- During this phase, you clearly scope your engagement. If you do not scope correctly, you will run into issues with your client (if you work as a consultant) or with your boss (if you are part of a corporate red team), and you might even encounter legal problems.

NOTE A ***red team*** is a group of cybersecurity experts and penetration testers hired by an organization to mimic a real threat actor by exposing vulnerabilities and risks regarding technology, people, and physical security. A ***blue team*** is a corporate security team that defends the organization against cybersecurity threats (that is, the security operation center analysts, computer security incident response teams [CSIRTs], information security [InfoSec] teams, and others).

Overview (Cont.)

Some key concepts you must address and understand in the planning and preparation phase:

- The target audience
- The rules of engagement
- The communication escalation path and communication channels
- The available resources and requirements
- The overall budget for the engagement
- Any specific disclaimers
- Any technical constraints
- The resources available to you as a penetration tester

Regulatory Compliance Considerations

You must be familiar with several regulatory compliance considerations in order to be successful in ethical hacking and penetration testing – not only to complete compliance-based assessments but also to understand what regulations may affect you and your client.

Regulation	Description
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) regulation aims to secure the processing of credit card payments and other types of digital payments.
HIPAA	• The original intent of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulation was to simplify and standardize healthcare administrative processes. • Administrative simplification called for the transition from paper records and transactions to electronic records and transactions. • The U.S. Department of Health and Human Services (HHS) was instructed to develop and publish standards to protect an individual's electronic health information while permitting appropriate access and use of that information by healthcare providers and other entities.
FedRAMP	The U.S. federal government uses the Federal Risk and Authorization Management Program (FedRAMP) standard to authorize the use of cloud service offerings.

Regulatory Compliance Considerations (Cont.)

- Most of these regulations and specifications require the regulated company to hire third-party penetration testing firms to make sure they are compliant and to ensure that their security posture is acceptable.
- You must be familiar with these regulations if you are hired to perform penetration testing to verify compliance and the overall security posture of the organization.
- Many of these standards provide checklists of the items that should be assessed during a penetration testing engagement.
- You must also become familiar with different privacy-related regulations, such as the General Data Protection Regulation (GDPR).
- GDPR includes strict rules around the processing of data and privacy.
- One of the GDPR's main goals is to strengthen and unify data protection for individuals within the European Union (EU), while addressing the export of personal data outside the EU.
- The primary objective of the GDPR is to give citizens control of their personal data.

Regulatory Compliance Considerations (Cont.)

Regulations in the Financial Sector

- Financial services institutions such as banks, credit unions, and lending institutions provide an array of solutions and financial instruments. Customer and transactional information is the heart of their business.
- Protection of customer information is necessary to establish and maintain trust between a financial institution and the community it serves.
- More specifically, institutions have a responsibility to safeguard the privacy of individual consumers and protect them from harm, including fraud and identity theft.
- On a broader scale, the industry is responsible for maintaining the critical infrastructure of the nation's financial services.

Regulatory Compliance Considerations (Cont.)

Examples of regulations applicable to the financial sector

- Title V, Section 501(b) of the Gramm-Leach-Bliley Act (GLBA) and the corresponding interagency guidelines
- The Federal Financial Institutions Examination Council (FFIEC)
- The Federal Deposit Insurance Corporation (FDIC) Safeguards Act and Financial Institutions Letters (FILs)
- The New York Department of Financial Services Cybersecurity Regulation (NY DFS Cybersecurity Regulation; 23 NYCRR Part 500)

Compliance with some regulations, such as NYCRR and GLBA, is mandatory.

Regulatory Compliance Considerations (Cont.)

- GLBA defines a financial institution as “any institution the business of which is significantly engaged in financial activities as described in Section 4(k) of the Bank Holding Company Act (12 U.S.C. § 1843(k)).” GLBA applies to all financial services organizations, regardless of size.
- This definition is important to understand because these financial institutions include many companies that are not traditionally considered to be financial institutions, including:
  - Check-cashing businesses
  - Payday lenders
  - Mortgage brokers
  - Nonbank lenders (for example, automobile dealers providing financial services)
  - Technology vendors providing loans to clients
  - Educational institutions providing financial aid
  - Debt collectors
  - Real estate settlement service providers
  - Personal property or real estate appraisers
  - Retailers that issue branded credit cards
  - Professional tax preparers
  - Courier services
- **The law also applies to companies that receive information about customers of other financial institutions, including credit reporting agencies and ATM operators.**

Regulatory Compliance Considerations (Cont.)

- The Federal Trade Commission (FTC) is responsible for enforcing GLBA as it pertains to financial firms that are not covered by federal banking agencies, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and state insurance authorities, which include tax preparers, debt collectors, loan brokers, real estate appraisers, and nonbank mortgage lenders. **GLBA mandates that financial organizations undergo periodic penetration testing in their infrastructure**.

- Another example is the NY DFS Cybersecurity Regulation. Section 500.05 of this regulation requires the covered entity to perform security penetration testing and vulnerability assessments on an ongoing basis. The cybersecurity program needs to include monitoring and testing, developed in accordance with the covered entity's risk assessment, which is designed to assess the effectiveness of the covered entity's cybersecurity program. The regulation dictates that "the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments." **The organization must conduct an annual security penetration testing and a biannual vulnerability assessment**.

Regulatory Compliance Considerations (Cont.)

Regulations in the Healthcare Sector

- On February 20, 2003, the Security Standards for the Protection of Electronic Protected Health Information, known as the **HIPAA Security Rule**, was published. The Security Rule requires technical and nontechnical safeguards to protect electronic health information. The corresponding HIPAA Security Enforcement Final Rule was issued on February 16, 2006. Since then, the following legislation has modified and expanded the scope and requirements of the Security Rule:
    - The 2009 Health Information Technology for Economic and Clinical Health Act (known as the HITECH Act)
    - The 2009 Breach Notification Rule
    - The 2013 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (known as the Omnibus Rule)

Regulatory Compliance Considerations (Cont.)

- HHS has published additional cybersecurity guidance to help healthcare professionals defend against security vulnerabilities, ransomware, and modern cybersecurity threats.
- The HIPAA Security Rule focuses on safeguarding electronic protected health information (ePHI), which is defined as individually identifiable health information (IIHI) that is stored, processed, or transmitted electronically.
- The HIPAA Security Rule applies to covered entities and business associates.
- Covered entities include healthcare providers, health plans, healthcare clearinghouses, and certain business associates.

Regulatory Compliance Considerations (Cont.)

Healthcare Provider	A person or an organization that provides patient or medical services, such as doctors, clinics, hospitals, and outpatient services; counseling; nursing home and hospice services; pharmacy services; medical diagnostic and imaging services; and durable medical equipment.
Healthcare Plan	An entity that provides payment for medical services, such as health insurance companies, HMOs, government health plans, or government programs that pay for healthcare, such as Medicare, Medicaid, military, and veterans' programs.
Healthcare Clearinghouse	An entity that processes nonstandard health information it receives from another entity into a standard format.
Business Associates	Business associates were initially defined as persons or organizations that perform certain functions or activities involving the use or disclosure of personal health information (PHI) on behalf of, or provide services to, a covered entity. Business associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services. Subsequent legislation expanded the definition of a business associate to a person or an entity that creates, receives, maintains, transmits, accesses, or has the potential to access PHI to perform certain functions or activities on behalf of a covered entity.

Regulatory Compliance Considerations (Cont.)

Payment Card Industry Data Security Standard (PCI DSS)

- In order to protect cardholders against misuse of their personal information and to minimize payment card channel losses, the major payment card brands (Visa, MasterCard, Discover, and American Express) formed the Payment Card Industry Security Standards Council (PCI SSC) and developed the Payment Card Industry Data Security Standard (PCI DSS).

- PCI DSS must be adopted by any organization that transmits, processes, or stores payment card data or that directly or indirectly affects the security of cardholder data. Any organization that leverages a third party to manage cardholder data has the full responsibility of ensuring that this third party is compliant with PCI DSS. The payment card brands can levy fines and penalties against organizations that do not comply with the requirements and/or can revoke their authorization to accept payment cards.

Regulatory Compliance Considerations (Cont.)

Key Terms Defined by PCI DSS	
Acquirer	Also referred to as an “acquiring bank” or an “acquiring financial institution,” an entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
ASV (approved scanning vendor)	An organization approved by the PCI SSC to conduct external vulnerability scanning services.
Merchant	An entity that accepts payment cards bearing the logos of any of the members of PCI SSC (American Express, Discover, MasterCard, or Visa) as payment for goods and/or services.
PAN (primary account number)	A payment card number that is up to 19 digits long.
Payment Brand	Brands such as Visa, MasterCard, Amex, or Discover.
PCI Forensic Investigator (PFI)	A person trained and certified to investigate and contain information about cybersecurity incidents and breaches involving cardholder data.

Regulatory Compliance Considerations (Cont.)

Key Terms Defined by PCI DSS (Continue)	
Qualified Security Assessor (QSA)	An individual trained and certified to carry out PCI DSS compliance assessments.
Service Provider	A business entity that is not a payment brand and that is directly involved in the processing, storage, or transmission of cardholder data. This includes companies that provide services that control or could impact the security of cardholder data, such as managed service providers that provide managed firewalls, intrusion detection and other services, and hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

To counter the potential for staggering losses, the payment card brands contractually require that all organizations that store, process, or transmit cardholder data and/or sensitive authentication data comply with PCI DSS. PCI DSS requirements apply to all system components where account data is stored, processed, or transmitted.

Regulatory Compliance Considerations (Cont.)

- PCI DSS requirements apply to all system components where *account data* is stored, processed, or transmitted.
- Account data consists of cardholder data as well as sensitive authentication data.
- The PAN is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements apply if the PAN is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

Cardholder Data	Sensitive Authentication Data
Primary account number (PAN)	Full magnetic stripe data or equivalent data on a chip
Cardholder name	CAV2/CVC2/CVV2/CID
Expiration date	PINs/PIB blocks
Service code	

Regulatory Compliance Considerations (Cont.)

- If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN or are otherwise present in the cardholder data environment, they too must be protected. Per the standards, the PAN must be stored in an unreadable (encrypted) format. Sensitive authentication data may never be stored post-authorization, even if encrypted.

- The Luhn algorithm, or Luhn formula, is an industry algorithm used to validate different identification numbers, including credit card numbers, International Mobile Equipment Identity (IMEI) numbers, national provider identifier numbers in the United States, Canadian Social Insurance Numbers, and more.

- Most credit cards and many government organizations use the Luhn algorithm to validate numbers. The Luhn algorithm is based on the principle of modulo arithmetic and digital roots. It uses modulo-10 mathematics.

Regulatory Compliance Considerations (Cont.)

Typical elements on the front of a credit card:

- Embedded microchip
- PAN
- Expiration date
- Cardholder name

The microchip contains the same information as the magnetic stripe. Most non-U.S. cards have a microchip instead of a magnetic stripe. Some U.S. cards have both for international acceptance.

Typical elements on the back of a credit card:

- **Magnetic stripe (mag stripe)**: The magnetic stripe contains encoded data required to authenticate, authorize, and process transactions.
- **CAV2/CID/CVC2/CVV2**: All these abbreviations are names for card security codes for the different payment brands.

Regulatory Compliance Considerations (Cont.)

Key Technical Elements in Regulations You Should Consider

Most regulations dictate several key elements, and a penetration tester should pay attention to and verify them during assessment to make sure the organization is compliant.

Data Isolation	Organizations that need to comply with PCI DSS (and other regulations, for that matter) should have a data isolation strategy. Also known as network isolation or network segmentation, the goal is to implement a completely isolated network that includes all systems involved in payment card processing.
Password Management	Most regulations mandate solid password management strategies. For example, organizations must not use vendor-supplied defaults for system passwords and security parameters. This requirement also extends far beyond its title and enters the realm of configuration management. In addition, most of these regulations mandate specific implementation standards, including password length, password complexity, and session timeout, as well as the use of multifactor authentication.
Key Management	A *key* is a value that specifies what part of the algorithm to apply and in what order, as well as what variables to input. It is critical to use a strong key that cannot be discovered and to protect the key from unauthorized access. Protecting the key is generally referred to as *key management*. NIST SP 800-57: Recommendations for Key Management, Part 1: General (Revision 4) provides general guidance and best practices for the management of cryptographic keying material. Part 2: Best Practices for Key Management Organization provides guidance on policy and security planning requirements for U.S. government agencies. Part 3: Application Specific Key Management Guidance provides guidance when using the cryptographic features of current systems.

Local Restrictions

- You should be aware of any local restrictions when you are hired to perform penetration testing.
- For instance, you may be traveling abroad to a different country where there may be specific country limitations and local laws that may restrict whether you can perform some tasks as a penetration tester.
- Penetration testing laws vary from country to country.
- Some penetration testers have been accused and even arrested for allegedly violating the Computer Fraud and Abuse Act of America Section 1030(a)(5)(B).
- You must always have clear documentation from your client (the entity that hired you) indicating that you have permission to perform the testing.
- Clearly, some of these limitations and considerations may have a direct impact to your contract and statement of work (SOW).

Local Restrictions (Cont.)

- During your pre-engagement tasks, you should identify testing constraints, including tool restrictions.
- Often you will be constrained by certain aspects of the business and the technology in the organization that hired you (even outlining the tools that you can use or are not authorized to use during the penetration testing engagement).

A few examples of constraints that you might face during a penetration testing engagement:

- Certain areas and technologies that cannot be tested due to operational limitations (For instance, you might not be able to launch specific SQL injection attacks, as doing so might corrupt a production database.)
- Technologies that might be specific for the organization being tested
- Limitation of skill sets
- Limitation of known exploits
- Systems that are categorized as out of scope because of the criticality or known performance problems

Local Restrictions (Cont.)

- You should clearly communicate any technical constraints with the appropriate stakeholders of the organization that hired you prior to and during the testing.
- You might also face different local government requirements such as the privacy requirements of GDPR and the California Consumer Privacy Act (CCPA), which is a state law focused on privacy.

Legal Concepts

There are several important legal concepts that you must know when performing a penetration test:

Service-level agreement (SLA)	A well-documented expectation or constraint related to one or more of the minimum and/or maximum performance measures (such as quality, timeline/timeframe, and cost) of the penetration testing service.
Confidentiality	You must discuss and agree on the handling of confidential data. For example, if you are able to find passwords or other sensitive data, do you need to disclose all those passwords or all that sensitive data? Who will have access to the sensitive data? What will be the proper way to communicate and handle such data? Similarly, you must protect sensitive data and delete all records, per your agreement with your client. Every time you finish a penetration testing engagement, you should delete any records from your systems.

Legal Concepts (Cont.)

There are several important legal concepts that you must know when performing a penetration test:

Statement of work (SOW)	A document that specifies the activities to be performed during a penetration testing engagement. It can be used to define some of the following elements: • Project (penetration testing) timelines, including the report delivery schedule • The scope of the work to be performed • The location of the work (geographic location or network location) • Special technical and nontechnical requirements • Payment schedule • Miscellaneous items that may not be part of the main negotiation but that need to be listed and tracked because they could pose problems during the overall engagement The SOW can be a standalone document or can be part of a ***master service agreement (MSA).***

Legal Concepts (Cont.)

There are several important legal concepts that you must know when performing a penetration test:

Master service agreement (MSA)	MSAs are contracts that can be used to quickly negotiate the work to be performed. When a master agreement is in place, the same terms do not have to be renegotiated every time you perform work for a customer. MSAs are especially beneficial when you perform a penetration test, and you know that you will be rehired on a recurring basis to perform additional tests in other areas of the company or to verify that the security posture of the organization has been improved as a result of prior testing and remediation.

Legal Concepts (Cont.)

There are several important legal concepts that you must know when performing a penetration test:

Non-disclosure agreement (NDA)	A legal document and contract between you and an organization that has hired you as a penetration tester. An NDA specifies and defines confidential material, knowledge, and information that should not be disclosed and that should be kept confidential by both parties. NDAs can be classified as any of the following: • **Unilateral**: With a unilateral NDA, only one party discloses certain information to the other party, and the information must be kept protected and not disclosed. For example, an organization that hires you should include in an NDA certain information that you should not disclose. • **Bilateral**: It is also referred to as a mutual, or two-way, NDA. In a bilateral NDA, both parties share sensitive information with each other, and this information should not be disclosed to any other entity. • **Multilateral**: It involves three or more parties, with at least one of the parties disclosing sensitive information that should not be disclosed to any entity outside the agreement. Multilateral NDAs are used in the event that an organization external to your customer (business partner, service provider, and so on) should also be engaged in the penetration testing engagement.

Contracts

- The contract is one of the most important documents in a pen testing engagement. It specifies the terms of the agreement and how you will get paid, and it provides clear documentation of the services that will be performed.
- A contract should be very specific, easy to understand, and without ambiguities. Any ambiguities will likely lead to customer dissatisfaction and friction.
- Legal advice (from a lawyer) is always recommended for any contract.
- Your customer might also engage its legal department or an outside agency to review the contract.
- A customer might specify and demand that any information collected or analyzed during the penetration testing engagement cannot be made available outside the country where you performed the test.
- In addition, the customer might specify that you (as the penetration tester) cannot remove personally identifiable information (PII) that might be subject to specific laws or regulations without first committing to be bound by those laws and regulations or without the written authorization of the company.
- Your customer will also review the penetration testing contract or agreement to make sure it does not permit more risk than it is intended to resolve.

Contracts (Cont.)

- Another very important element of your contract and pre-engagement tasks is that you must obtain a signature from a proper signing authority for your contract.
- This includes written authorization for the work to be performed.
- If necessary, you should also have written authorization from any third-party provider or business partner.
- This would include, for example, Internet service providers, cloud service providers, or any other external entity that could be impacted by or related to the penetration test to be performed.

Disclaimers

- You might want to add disclaimers to your pre-engagement documentation, as well as in the final report.
- For example, you can specify that you conducted penetration testing on the applications and systems that existed as of a clearly stated date. Cybersecurity threats are always changing, and new vulnerabilities are discovered daily. No software, hardware, or technology is immune to security vulnerabilities, no matter how much security testing is conducted.
- You should also specify that the penetration testing report is intended only to provide documentation and that your client will determine the best way to remediate any vulnerabilities. In addition, you should include a disclaimer that your penetration testing report cannot and does not protect against personal or business loss as a result of use of the applications or systems described therein.
- Another standard disclaimer is that you (or your organizations) provide no warranties, representations, or legal certifications concerning the applications or systems that were or will be tested. A disclaimer might say that your penetration testing report does not represent or warrant that the application tested is suitable to the task and free of other vulnerabilities or functional defects aside from those reported. In addition, it is standard to include a disclaimer stating that such systems are fully compliant with any industry standards or fully compatible with any operating system, hardware, or other application.

Lab - Compliance Requirements and Local Restrictions

In this lab, you will complete the following objectives:

- Research penetration testing services provided by security consultants for compliance frameworks.
- Conduct a Search of Penetration Testing Companies.

2.2 Explaining the Importance of Scoping and Organizational or Customer Requirements

Overview

- In Module 1, “Introduction to Ethical Hacking and Penetration Testing,” you learned about the importance of a written permission to attack and the different penetration testing standards and methodologies, such as the Penetration Testing Execution Standard (PTES), the Open Source Security Testing Methodology Manual (OSSTMM), the Information Systems Security Assessment Framework (ISSAF), and different guidance documents from the National Institute of Standards and Technology (NIST) and the Open Web Application Security Project (OWASP).

- You also learned about the different environmental considerations (for network, application, and cloud environments).

- In this section you will learn about rules of engagement, target list/in-scope assets, and how to validate the scope of an engagement.

Rules of Engagement

- The **rules of engagement document** specifies the conditions under which the security penetration testing engagement will be conducted. You need to document and agree upon these rule of engagement conditions with the client or an appropriate stakeholder.

Table 2-3 Sample Elements of a Rules of Engagement Document

Rule of Engagement Element	Example
Testing timeline	Three weeks. As specified in a Gantt chart
Location of the testing	Company's headquarters in Raleigh, North Carolina
Time window of the testing (time of day)	9:00 a.m. to 5:00 p.m. EST
Preferred method of communication	Final report and weekly status update meetings

Rules of Engagement (Cont.)

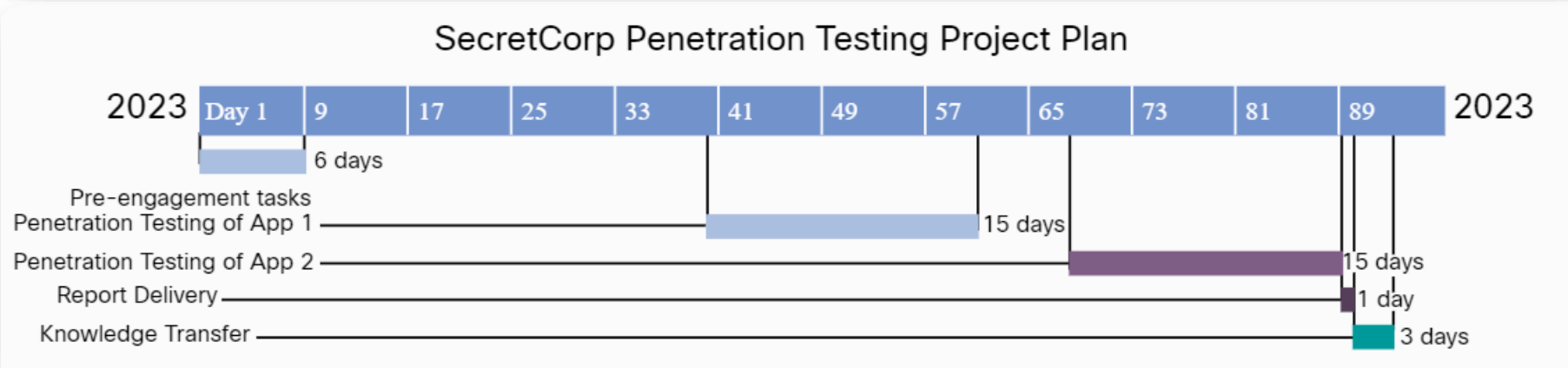
Table 2-3 Sample Elements of a Rules of Engagement Document (Continue)

Rule of Engagement Element	Example
The security controls that could potentially detect or prevent testing	Intrusion prevention systems (IPSs), firewalls, data loss prevention (DLP) systems
IP addresses or networks from which testing will originate	10.10.1.0/24, 192.168.66.66, 10.20.15.123
Types of allowed or disallowed tests	Testing only web applications (app1.secretcorp.org and app2.secretcorp.org). No social engineering attacks are allowed. No SQL injection attacks are allowed in the production environment. SQL injection is only allowed in the development and staging environments at: app1-dev.secretcorp.org app1-stage.secretcorp.org app2-dev.secretcorp.org app2-stage.secretcorp.org

Rules of Engagement (Cont.)

Gantt charts and work breakdown structures (WBS) can be used as tools to demonstrate and document the timeline.

Figure 2-1 Example of a Gantt Chart



Target List and In-Scope Assets

- Scoping is one of the most important elements of the pre-engagement tasks with any penetration testing engagement.
- You not only have to carefully identify and document all systems, applications, and networks that will be tested but also determine any specific requirements and qualifications needed to perform the test.
- The broader the scope of the penetration testing engagement, the more skills and requirements that will be needed.
- Your scope and related documentation must include information about what types of networks will be tested.
- In addition to IP ranges, you must document any wireless networks or service set identifiers (SSIDs) that you are allowed or not allowed to test.
- You may also be hired to perform an assessment of modern applications using different application programming interfaces (APIs).

Target List and In-Scope Assets (Cont.)

Types of API Documentation:

Simple Object Access Protocol (SOAP)	SOAP is an API standard that relies on XML and related schemas. XML-based specifications are governed by XML Schema Definition (XSD) documents. Having a good reference of what a specific API supports can be very beneficial for a penetration tester and will accelerate the testing.
Swagger	Swagger (OpenAPI) documentation is a modern framework of API documentation and development that is now the basis of the OpenAPI Specification (OAS). These documents are used in representational state transfer (REST) APIs. REST is a software architectural style designed to guide development of the architecture for web services (including APIs). REST, or "RESTful," APIs are the most common types of APIs used today. Swagger documents can be extremely beneficial when testing APIs.
WSDL	Web Services Description Language (WSDL) is an XML-based language that is used to document the functionality of a web service.

Target List and In-Scope Assets (Cont.)

Types of API Documentation (Continue):

GraphQL	GraphQL is a query language for APIs. It is also a server-side runtime for executing queries using a type system you define for your data.
WADL	Web Application Description Language (WADL) is an XML-based language for describing web applications.
WSDL	Web Services Description Language (WSDL) is an XML-based language that is used to document the functionality of a web service.

Target List and In-Scope Assets (Cont.)

Additional support resources that you might obtain from the organization that hired you to perform the penetration test:

Software development kit (SDK) for specific applications	An SDK, or devkit, is a collection of software development tools that can be used to interact and deploy a software framework, an operating system, or a hardware platform. SDKs can also help pen testers understand certain specialized applications and hardware platforms within the organization being tested.
Source code access	Some organizations may allow you to obtain access to the source code of applications to be tested.
Examples of application requests	In most cases, you will be able to reveal context by using web application testing tools such as proxies like the Burp Suite and the OWASP Zed Attack Proxy (ZAP).
System and network architectural diagrams	These documents can be very beneficial for penetration testers, and they can be used to document and define what systems are in scope during the testing.

Target List and In-Scope Assets (Cont.)

- It is very important to document the physical location where the penetration testing will be done, as well as the Domain Name System (DNS) fully qualified domain names (FQDNs) of the applications and assets that are allowed (including any subdomains).
- You must also agree and understand if you will be allowed to demonstrate how an external attacker could compromise your systems or how an insider could compromise internal assets.
- This external vs. internal target identification and scope should be clearly documented.
- Applications today can not only be hosted in one public cloud (such as AWS, GCP, or Azure) but also in private and hybrid clouds.
- As a penetration tester, you must become familiar with any restrictions and limitations dictated by any third-party hosting or cloud providers.
- ***Scope creep*** is a project management term that refers to the uncontrolled growth of a project's scope. It is also often referred to as *kitchen sink syndrome, requirement creep* , and *function creep*. Scope creep can put you out of business.
- Many security firms suffer from scope creep and are unsuccessful because they have no idea how to identify when the problem starts or how to react to it.

Target List and In-Scope Assets (Cont.)

Situations in which a scope creep might occur:

Change Management	When there is poor change management in the penetration testing engagement.
Technical and Nontechnical Elements	When there is ineffective identification of what technical and nontechnical elements will be required for the penetration test.
Poor Communication	When there is poor communication among stakeholders, including your client and your own team.

- Scope creep does not always start as a bad situation. For example, a client that is satisfied with the work you are doing in your engagement might ask you to perform additional testing or technical work.
- Change management and clear communication are crucial to avoid a very uncomfortable and bad situation.
- If you initially engaged with your client after a request for proposal (RFP), and additional work is needed that was not part of the RFP or your initial SOW, you should ask for a new SOW to be signed and agreed upon.

Validating the Scope of Engagement

- The first step in validating the scope of an engagement is to question the client and review contracts.
- You must also understand who the target audience is for your penetration testing report.
- You should understand the subjects, business units, and any other entity that will be assessed by such a penetration testing engagement.

Questions to ask for discovering different characteristics of target audience:

First question	What is the entity's or individual's need for the report?
Primary recipient of the report	What is the position of the individual who will be the primary recipient of the report within the organization?
Purpose and goal	What is the main purpose and goal of the penetration testing engagement and ultimately the purpose of the report?
Responsibility and authority	What is the individual's or business unit's responsibility and authority to make decisions based on your findings?
Report address to	Who will the report be addressed to–for example, the information security manager (ISM), chief information security officer (CISO), chief information officer (CIO), chief technical officer (CTO), technical teams, and so on?
Others with access to the report	Who will have access to the report, which may contain sensitive information that should be protected, and whether access will be provided on a need-to-know basis?

Validating the Scope of Engagement (Cont.)

You should always have good open lines of communication with the clients and the stakeholders that hire you.

You should have proper documentation of answers to the following questions.

Relevant stakeholders	What is the contact information for all relevant stakeholders?
Communication process	How will you communicate with the stakeholders?
Timing of interactions	How often do you need to interact with the stakeholders?
Emergency contacts	Who are the individuals you can contact at any time if an emergency arises?

Validating the Scope of Engagement (Cont.)

Figure 2-2 - Stakeholder and Emergency Contact Card Example

PRIMARY STAKEHOLDER

Name | Email

Title | Responsibility

Work Number | Mobile Phone | Other Number | Alternate Email

Address | Notes

City | State | ZIP Code

EMERGENCY CONTACTS

Primary Emergency Contact | Secondary Emergency Contact

Phone | Email | Phone | Email

Address | Address

City, ST ZIP Code | City, ST ZIP Code

Validating the Scope of Engagement (Cont.)

- You should ask for a form of secure bulk data transfer or storage, such as Secure Copy Protocol (SCP) or Secure File Transfer Protocol (SFTP).
- You should also exchange any Pretty Good Privacy (PGP) keys or Secure/Multipurpose Internet Mail Extensions (S/MIME) keys for encrypted email exchanges.

- Questions about budget and return on investment (ROI) may arise from both the client side and the tester sides in penetration testing.

Clients may ask such questions:

Cost justification	How do I explain the overall cost of penetration testing to my boss?
Need for penetration testing	Why do we need penetration testing if we have all these security technical and nontechnical controls in place?
Success factor	How do I build in penetration testing as a success factor?
Need for external vendor	Can I do it myself?
Return on investment (ROI)	How do I calculate the ROI for the penetration testing engagement?

Validating the Scope of Engagement (Cont.)

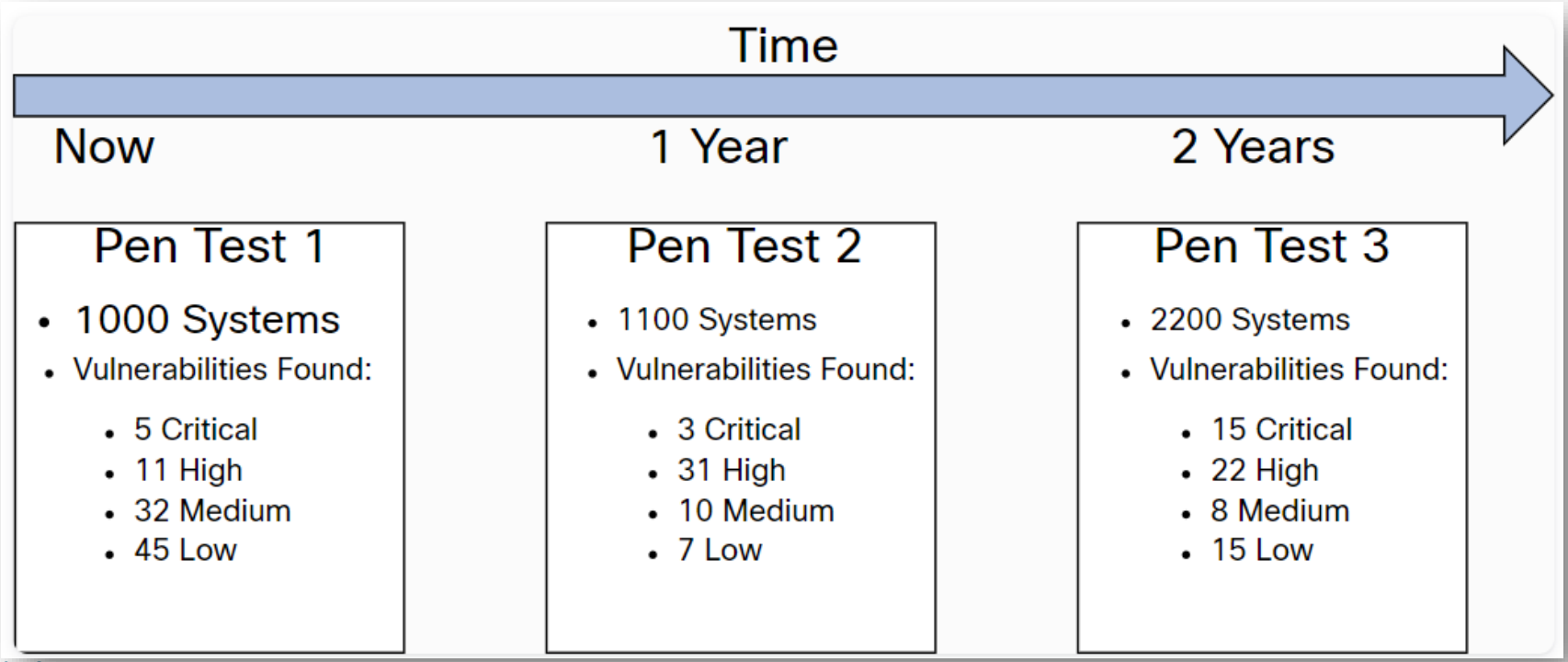
At the same time, the tester needs to answer questions like these:

Budget concerns	How do I account for all items of the penetration testing engagement to avoid going over budget?
Pricing	How do I do pricing?
Demonstrate ROI	How can I clearly show ROI to my client?

- The answers to these questions depend on how effective you are at scoping and clearly communicating and understanding all the elements of the penetration testing engagement.
- Another factor is understanding that penetration testing is a point-in-time assessment.

Validating the Scope of Engagement (Cont.)

Figure 2-3 – Point-in-Time Assessment



Validating the Scope of Engagement (Cont.)

- In Figure 2-3, a total of three pen testing engagements took place in a period of two years at the same company.
- In the first engagement, 1000 systems were assessed; 5 critical-, 11 high-, 32 medium-, and 45 low-severity vulnerabilities were uncovered.
- A year later, 1100 systems were assessed; 3 critical-, 31 high-, 10 medium-, and 7 low-severity vulnerabilities were uncovered.
- Then two years later, 2200 systems were assessed; 15 critical-, 22 high-, 8 medium-, and 15 low-severity vulnerabilities were uncovered.
- Is the company doing better or worse?
- Are the pen test engagements done just because of a compliance requirement?
- How can you justify the penetration testing if you continue to encounter vulnerabilities over and over after each engagement?

Validating the Scope of Engagement (Cont.)

- You can see that it is important for both the client and the pen tester to comprehend that penetration testing alone cannot guarantee the overall security of the company.
- The pen tester also needs to incorporate clear and achievable mitigation strategies for the vulnerabilities found.
- In addition, an appropriate impact analysis and remediation timelines must be discussed with the respective stakeholders.

Strategy: Unknown vs. Known Environment Testing

- When talking about penetration testing strategies, you are likely to hear the terms ***unknown-environment testing*** and ***known-environment testing*** that are used to describe the perspective from which the testing is performed, as well as the amount of information that is provided to the tester.

Unknown-Environment Testing (formerly referred to as **black-box** penetration testing)	In this type of testing, the tester is typically provided only a very limited amount of information. For instance, the tester may be provided only the domain names and IP addresses that are in scope for a particular target. The idea of this type of limitation is to have the tester start out with the perspective that an external attacker might have. Typically, an attacker would first determine a target and then begin to gather information about the target, using public information, and gaining more and more information to use in attacks. The tester would not have prior knowledge of the target's organization and infrastructure. Another aspect of unknown-environment testing is that sometimes the network support personnel of the target may not be given information about exactly when the test is taking place. This allows for a defense exercise to take place, and it also eliminates the issue of a target preparing for the test and not giving a real-world view of the security posture.
Known-Environment Testing (formerly known as **white-box** penetration testing)	In this type of testing, the tester starts out with a significant amount of information about the organization and its infrastructure. The tester is normally provided things like network diagrams, IP addresses, configurations, and a set of user credentials. If the scope includes an application assessment, the tester might also be provided the source code of the target application. The idea of this type of testing is to identify as many security holes as possible.

Strategy: Unknown vs. Known Environment Testing (Cont.)

- In a known-environment test, the scope might be only to identify a path into the organization and stop there.
- With unknown-environment testing, the scope would typically be much broader and would include internal network configuration auditing and scanning of desktop computers for defects.
- Time and money are typically deciding factors in the determination of which type of penetration test to complete.
- If a company has specific concerns about an application, a server, or a segment of the infrastructure, it can provide information about that specific target to decrease the scope and the amount of time spent on the test but still uncover the desired results.

Lab - Pre-Engagement Scope and Planning

Obtaining agreement on the rules of engagement that apply to a penetration test or security audit is the first step in any engagement with a client. It is important to spend the time to ensure that both your firm and the client have a clear understanding of the terms and scope of the testing engagement.

- Create a penetration test scope and plan document that addresses the requirements for penetration testing services that were gathered from the client.
- Determine the rules of engagement elements.

Lab - Create a Pen testing Agreement

In this lab, you will complete the following objectives:

- Complete a simple pen testing agreement.

2.3 Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity

Overview

There are many scenarios in which an ethical hacker (penetration tester) should demonstrate professionalism and integrity.

Background checks of penetration testing teams	A client may require that you and your team undergo careful background checks, depending on the environment and engagement. Organizations sometimes require these background checks to feel comfortable with the penetration testing teams that they are allowing to access their environment and information. Your clients may check your credentials and make sure that you have the skills to make their network more secure by finding vulnerabilities that could be exploited by malicious attackers.
Identification of criminal activity and immediate reporting of breaches/criminal activities	In some cases, you may find that a real attacker has already compromised the client's systems and network. In such cases, you must identify any criminal activities and report them immediately.

Overview (Cont.)

Adherence to the specific scope of engagement	You have already learned about the importance of proper scoping of the penetration testing engagement. There might be company-specific scoping elements that you need to take into consideration. For example, you might have been hired to perform a penetration test of a company that is being acquired by the company that hired you, as part of the pre-merger process. For example, the acquiring company might ask the company that is being acquired to show whether penetration testing has been conducted in the past year or the past six months. If not, the company being acquired might be required to hire a penetration testing firm to perform an assessment. During the scoping phase, the target selection process needs to be carefully completed with the company that hired you, or, if you are part of a full-time red team, with the appropriate stakeholders in your organization. The organization might create a list of applications, systems, or networks to be tested. This is often referred to as a penetration testing scope "allow list." An allow list is a list of applications, systems, or networks that are in scope and should be tested. On the other hand, a deny list is a list of applications, systems, or networks that are not in scope and should not be tested. You must always obey those rules.

Overview (Cont.)

Limiting the use of tools to particular engagement	In some penetration testing engagements, you will not be allowed to use a particular set of tools that the organization does not permit because of legal reasons or because those tools could bring down the network and underlying systems.
Limiting invasiveness based on scope	After the penetration tester and the client or appropriate stakeholder agree on the scope of the test, the penetration tester could do target discovery by performing active and passive reconnaissance. In Module 3, "Information Gathering and Vulnerability Identification," you will learn how to perform information gathering and reconnaissance, how to conduct and analyze vulnerability scans, and how to leverage reconnaissance results to prepare for the exploitation phase. Some tools and attacks could be detrimental and extremely disruptive for your client's systems and mission. You should always limit the verbosity and invasiveness of your tests and tools based on the agreed scope.

Overview (Cont.)

Confidentiality of data/information	The results of the penetration testing engagement (report) and the information that you may gather and have access to during the penetration testing engagement must be protected and kept confidential. If this information is lost or shared, it could be used by an adversary to cause a lot of damage to your client.
Risks to the professional	If you do not adhere to the best practices outlined in this list, you could be subject to different fees or fines and, in some cases, even criminal charges. Therefore, companies and individuals conducting professional penetration testing often have at least general business liability insurance. If you are in the cybersecurity field (often dealing with risk management), you need to know the risks to your business and protect yourself against this risk.

Overview (Cont.)

- In order to have a strong cybersecurity program, you need to ensure that business objectives take into account risk tolerance and that the resulting policies are enforced and adopted.
- *Risk tolerance* is how much of an undesirable outcome a risk-taker is willing to accept in exchange for the potential benefit.
- Inherently, risk is neither good nor bad. All human activity carries some risk, although the amount varies greatly.
- Consider this: Every time you get in a car, you are risking injury or even death. You manage the risk by keeping your car in good working order, wearing a seatbelt, obeying the rules of the road, avoiding texting while driving, driving only when not impaired, and paying attention.
- You tolerate the risks because the reward for reaching your destination outweighs the potential harm.

Overview (Cont.)

- Risk-taking can be beneficial and is often necessary for advancement.
- For example, entrepreneurial risk-taking can pay off in innovation and progress.
- Ceasing to take risks would quickly wipe out experimentation, innovation, challenge, excitement, and motivation.
- Risk-taking can, however, be detrimental when it is influenced by ignorance, ideology, dysfunction, greed, or revenge.
- The key is to balance risk against rewards by making informed decisions and then managing the risk while keeping in mind organizational objectives.
- The process of managing risk requires organizations to assign risk management responsibilities, determine the organizational risk appetite and tolerance, adopt a standard methodology for assessing risk, respond to risk levels, and monitor risk on an ongoing basis.

Overview (Cont.)

- *Risk management* is the process of determining an acceptable level of risk (risk appetite and tolerance), calculating the current level of risk (risk assessment), accepting the level of risk (risk acceptance), or taking steps to reduce risk to an acceptable level (risk mitigation).
- Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process.
- Generally, but not always, this means that the outcome of the risk assessment is within tolerance.
- There might be times when the risk level is not within tolerance, but the organization will still choose to accept the risk because all other alternatives are unacceptable.
- Exceptions should always be brought to the attention of management and authorized by either the executive management or the board of directors.

Lab - Personal Code of Conduct

In this lab, you will complete the following objectives:

- Research Approaches to Ethical Decision Making
- Research Code of Ethics
- Develop Your Own Personal Code of Ethical Conduct

2.4 Planning and Scoping a Penetration Testing Assessment Summary

What Did I Learn in this Module?

Comparing and Contrasting Governance, Risk, and Compliance Concepts

- The planning and preparation phase is crucial in any penetration testing engagement and involves scoping the project properly.
- This includes understanding the target audience, rules of engagement, communication channels, available resources, budget, technical constraints, and any disclaimers.
- In addition, it is essential to be familiar with various regulatory compliance considerations, including PCI DSS, HIPAA, FedRAMP, and GDPR.
- Most of these regulations require third-party penetration testing to verify compliance and assess the security posture of the organization.
- It is important to be familiar with these regulations and their checklists for a successful compliance-based assessment.

What Did I Learn in this Module? (Cont.)

Regulations in the Financial Sector

- The financial sector is responsible for safeguarding customer information and maintaining the critical infrastructure of financial services.

- Regulations applicable to the financial sector include the Gramm-Leach-Bliley Act (GLBA), the Federal Financial Institutions Examination Council (FFIEC), the Federal Deposit Insurance Corporation (FDIC) Safeguards Act, and the New York Department of Financial Services Cybersecurity Regulation (NY DFS Cybersecurity Regulation).

- GLBA applies to all financial services organizations, including non-traditional financial institutions such as check-cashing businesses, payday lenders, and technology vendors providing loans to clients.

What Did I Learn in this Module? (Cont.)

Regulations in the Financial Sector (Continue)

- Compliance with some regulations, such as GLBA and NY DFS Cybersecurity Regulation, is mandatory.
- The regulations mandate financial institutions to undergo periodic penetration testing and vulnerability assessments in their infrastructure.
- The Federal Trade Commission (FTC) is responsible for enforcing GLBA as it pertains to financial firms not covered by federal banking agencies, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and state insurance authorities.

What Did I Learn in this Module? (Cont.)

Regulations in the Healthcare Sector

- The HIPAA Security Rule, published in 2003, requires technical and nontechnical safeguards to protect electronic health information.
- Since then, several legislations have modified and expanded the scope and requirements of the Security Rule, including the HITECH Act, the Breach Notification Rule, and the Omnibus Rule.
- The Security Rule applies to covered entities and business associates, including healthcare providers, health plans, healthcare clearinghouses, and certain business associates.
- HHS has published additional cybersecurity guidance to help healthcare professionals defend against security vulnerabilities, ransomware, and modern cybersecurity threats.
- HHS has also provided guidance material for the HIPAA Security Rule at their website.

What Did I Learn in this Module? (Cont.)

Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Security Standards Council (PCI SSC) was formed by major payment card brands (Visa, MasterCard, Discover, and American Express) to develop the Payment Card Industry Data Security Standard (PCI DSS) in order to protect cardholders against misuse of their personal information and to minimize payment card channel losses.
- PCI DSS must be adopted by any organization that transmits, processes, or stores payment card data or that directly or indirectly affects the security of cardholder data.
- Any organization that leverages a third party to manage cardholder data has the full responsibility of ensuring that this third party is compliant with PCI DSS.
- The Luhn algorithm is used to validate credit card numbers and other identification numbers.

What Did I Learn in this Module? (Cont.)

Key Technical Elements in Regulations You Should Consider

- Several key technical elements are mandated by most regulations, including data isolation, password management, and key management.
- Data isolation involves creating a separate network for systems involved in payment card processing to ensure they are completely isolated.
- Password management strategies must meet specific implementation standards and should include the use of strong passwords and multifactor authentication.
- Key management is also critical and involves the proper management and protection of cryptographic keys to ensure the security of information protected by cryptography.
- Policies and standards for key management should include assigned responsibilities, the nature of information to be protected, the classes of threats, and the cryptographic protection mechanisms to be used.

What Did I Learn in this Module? (Cont.)

Key Technical Elements in Regulations You Should Consider

- Several key technical elements are mandated by most regulations, including data isolation, password management, and key management.
- Data isolation involves creating a separate network for systems involved in payment card processing to ensure they are completely isolated.
- Password management strategies must meet specific implementation standards and should include the use of strong passwords and multifactor authentication.
- Key management is also critical and involves the proper management and protection of cryptographic keys to ensure the security of information protected by cryptography.
- Policies and standards for key management should include assigned responsibilities, the nature of information to be protected, the classes of threats, and the cryptographic protection mechanisms to be used.

What Did I Learn in this Module? (Cont.)

Legal Considerations

- Important legal concepts that are relevant to performing a penetration test include Service-level Agreements (SLAs), confidentiality agreements, statements of work (SOWs), master service agreements (MSAs), and non-disclosure agreements (NDAs).
- The section also emphasizes the importance of contracts in a penetration testing engagement and the need for clarity, specificity, and legal advice.
- Finally, it suggests adding disclaimers to pre-engagement documentation and final reports to address the limitations of penetration testing and to avoid potential legal liabilities.

What Did I Learn in this Module? (Cont.)

Explaining the Importance of Scoping and Organizational or Customer Requirements

- The rules of engagement document outlines the conditions under which the testing will be performed and includes details such as the testing timeline, location of testing, time window of testing, preferred method of communication, security controls that could potentially prevent testing, IP addresses or networks from which testing will originate, and types of allowed or disallowed tests.
- Gantt charts and work breakdown structures can be used to document the timeline of the testing.
- Scoping is one of the most important elements of the pre-engagement tasks and includes documentation of the systems, networks, and applications to be tested, as well as any specific requirements needed for the test.
- There are different types of API documentation and additional support resources that might be available for the penetration tester.
- The engagement scope must include physical location, DNS fully qualified domain names, and external vs. internal target identification.

What Did I Learn in this Module? (Cont.)

Explaining the Importance of Scoping and Organizational or Customer Requirements

- It is important to validate the scope of a penetration testing engagement and understand the target audience for the report.
- The topic provides a list of questions that can help discover different characteristics of the target audience, such as their need for the report, their position within the organization, and their responsibility and authority to make decisions based on the findings.
- It is also important to maintain open lines of communication with clients and stakeholders.
- The topic provides a list of questions to consider when communicating with stakeholders.
- Also, there may be questions about budget and return on investment that may arise from both the client and the tester sides in penetration testing.
- Make sure that the client understands that penetration testing is a point-in-time assessment and that clear and achievable mitigation strategies, impact analysis, and remediation timelines must be discussed with all stakeholders.

What Did I Learn in this Module? (Cont.)

Explaining the Importance of Scoping and Organizational or Customer Requirements

- **Unknown-environment testing** involves giving the tester only limited information, such as domain names and IP addresses, to simulate the perspective of an external attacker.
- The tester does not have prior knowledge of the target's organization and infrastructure, and the network support personnel of the target may not be informed about the test.
- This allows for a realistic assessment of the security posture.
- **Known-environment testing**, on the other hand, provides the tester with a significant amount of information about the organization and its infrastructure, including network diagrams, IP addresses, configurations, and user credentials. In some cases, the tester may also be provided with the source code of the target application. The goal of this type of testing is to identify as many security holes as possible.
- The scope of the test and the amount of time and money spent on it depends on various factors, such as the company's specific concerns and the level of sophistication and capabilities of potential attackers.
- While known-environment testing can be useful for identifying specific vulnerabilities, unknown-environment testing is often a good choice because it provides a more realistic assessment of the network's security posture.

What Did I Learn in this Module? (Cont.)

Demonstrating an Ethical Hacking Mindset by Maintaining Professionalism and Integrity

- This topic discusses several key considerations for ethical hackers or penetration testers to demonstrate professionalism and integrity.
- These include undergoing background checks, adhering to the specific scope of engagement, identifying criminal activity and reporting it immediately, limiting tool usage, respecting invasiveness based on scope, maintaining confidentiality of data and information, and understanding the risks involved.
- Additionally, the topic emphasizes the importance of risk management and risk tolerance in cybersecurity governance programs.
- All parties involved should make informed decisions and manage risk while keeping organizational objectives in mind.