Audits and Assessments

Objective 5.5: Explain types and purposes of audits and assessments

- **Audits and Assessments**
  - *Audits*
    - Systematic evaluations of an organization's information systems, applications, and security controls
    - Types
      - *Internal Audits*
        - Conducted by the organization's own team
      - *External Audits*
        - Performed by third-party entities
    - Purpose
      - Validate security measures
      - Identify vulnerabilities
      - Maintain compliance with regulatory standards
    - Examples
      - Internal Audit Example
        - Review of data protection policies
        - Check policy relevance and compliance
      - External Audit Example
        - Evaluation of e-commerce PCI DSS compliance
        - Assess network security, data encryption, and access controls

- Significance of Audits
    - Identifying Gaps
        - Security policies, procedures, and controls
    - Ensuring Compliance
        - GDPR, HIPAA, PCI DSS

- *Assessments*
    - Detailed analysis to identify vulnerabilities and risks
    - Performed before implementing new systems or significant changes
    - Categories
        - Risk Assessments
        - Vulnerability Assessments
        - Threat Assessments
- *Internal Audits and Assessments*
    - Review processes, controls, and compliance
    - Importance
        - Ensure operational effectiveness and adherence to internal policies
- *External Audits and Assessments*
    - Independent evaluations by external parties
    - Verification Areas
        - Financial statements
        - Compliance
        - Operational practices
- *Penetration Testing*
    - Simulated cyber attacks to identify vulnerabilities
    - Objective
        - Find vulnerabilities exploited by attackers

        - Also known as “Pen Testing” or “Ethical Hacking”
    - *Reconnaissance in Pentesting*
        - Gathering information before a pentest
        - Types
            - Passive
            - Active
        - Environment Consideration
            - Known
            - Partially Known
            - Unknown
    - *Attestation of Findings*
        - Formal, written declaration of audit or assessment results
        - Purpose
            - Confirmation and documentation of outcomes

- **Internal Audits and Assessments**
    - *Internal Audits*
        - Systematic evaluations conducted by an organization's own audit team
        - Assess the effectiveness of internal controls, compliance with regulations, and the integrity of information systems and processes
        - Focus areas may include
            - Data protection
            - Network security
            - Access controls
            - Incident response procedures

- Examples of internal audit focus areas
  - Password policies
  - User access controls
- Process
  - Reviewing policies and procedures
  - Examining access rights
  - Testing effectiveness of controls
  - Findings documented for recommendations and improvements
- Concepts in Internal Audits
  - *Compliance Requirements*
    - Ensuring adherence to established standards, regulations, and laws
    - Compliance is essential for protecting sensitive data and avoiding legal penalties
    - Internal audits may be required for compliance with specific laws or regulations
  - *Audit Committee*
    - A group, often comprising members of a company's board of directors, overseeing audit and compliance activities
    - Responsibilities
      - Reviewing financial reporting
      - Internal controls
      - Internal and external audits
      - Legal and regulatory compliance
    - Addresses issues raised by auditors

- *Internal Assessments*
  - Conducted to identify and evaluate potential risks and vulnerabilities in an organization's information systems
  - Commonly performed before implementing new systems or making significant changes to existing ones
  - *Self-assessments*
    - Internal evaluations assessing compliance with specific standards or regulations
  - Vulnerability assessments, threat modeling exercises, and risk assessments are part of internal assessments
  - Assisted internal assessments may involve dedicated assessment groups
  - Internal Assessment Process
    - *Threat Modeling Exercise*
      - Identifies potential threats to applications (e.g., SQL injection, XSS, DoS attacks)
    - *Vulnerability Assessment*
      - Uses automated scanning tools and manual testing techniques to identify known vulnerabilities and code weaknesses
    - *Risk Assessment*
      - Evaluates the potential impact of the following
        - Identified threats and vulnerabilities
        - Considering likelihood
        - Potential damage
        - Cost of security measures
  - Mitigation Strategies
    - Recommendations to address risks and vulnerabilities

    - Code fixes
    - Additional security controls
    - Architectural changes

- **Performing an Internal Assessment**
    - *Internal Assessment*
        - Proactive evaluation of an organization's security posture
        - Helps to identify and address potential risks and vulnerabilities in information systems
    - Using a Sample Checklist
        - The specific checklists and procedures for an internal assessment may vary based on the following
            - Organization's governance
            - Risk
            - Compliance practices
        - A sample checklist from the Minnesota Counties Intergovernmental Trust (MCIT) is used
        - *MCIT Cybersecurity Self-Assessment*
            - MCIT's Cybersecurity Self-Assessment checklist is designed to help organizations minimize data and cybersecurity-related exposures
            - It assists in identifying areas where data security may need strengthening
            - The checklist comprises yes-or-no questions with sections for comments and action items
            - Action items are assigned to specific individuals or groups responsible for implementing corrective actions

- Collaborative Approach
  - To maximize the checklist's effectiveness, involve a diverse group of participants from across the organization
    - Administration team
    - Information technology staff
    - Cybersecurity professionals
- Overview of the Checklist
  - The checklist is broad and aims to provide a quick overview of the organization's current risk posture
  - Organizations may use different checklists or variations with distinct questions
  - The general format and purpose of self-assessments are consistent across most organizations

- **External Audits and Assessments**
  - *External Audits and Assessments*
    - Essential tools for maintaining a robust security posture and ensuring regulatory compliance
    - Conducted by independent third parties to provide an unbiased perspective on an organization's security
  - *External Audits*
    - Systematic evaluations conducted by independent entities
    - Assess information systems, applications, and security controls
    - Focuses on various areas
      - Data protection
      - Network security
      - Access controls

- Incident response procedures
- Objective is to identify gaps in security policies and controls for compliance with regulatory standards such as
  - GDPR
  - HIPAA
  - PCI DSS

- *External Assessments*
  - Detailed analysis by independent entities to identify vulnerabilities and risks in an organization's security systems
  - Utilize automated scanning tools and manual testing techniques
  - External assessments can take various forms
    - Risk assessments
    - Vulnerability assessments
    - Threat assessments
- Regulatory Compliance
  - The goal is to ensure organizations comply with relevant laws, policies, and regulations
  - Organizations adopt consolidated and harmonized sets of compliance controls to achieve regulatory compliance, e.g., NIST Cybersecurity Framework
  - Compliance includes adherence to industry-specific rules (e.g., HIPAA, PCI DSS) and more generalized regulations like GDPR
- *Examinations*
  - Detailed inspections of an organization's security infrastructure conducted externally
  - Cover various areas
    - Network security

        - Data protection
        - Access controls
    - May include testing of the following
        - Key personnel
        - Certifications
        - Standardized assessments
    - Crucial for maintaining a strong security posture and regulatory compliance.
- Independent Third-Party Audits
    - Provide an unbiased perspective on an organization's security posture
    - Validate security measures and build trust with
        - Customers
        - Stakeholder
        - Regulatory bodies
    - Required by regulations like GDPR and PCI DSS for organizations to undergo regular independent third-party audits

- **Performing an External Assessment**
    - *External Assessment*
        - Part of maintaining a robust security posture and ensuring compliance
        - May vary based on the following
            - Organization's governance
            - Risk
            - Compliance practices
        - Sample checklist used for a HIPAA external assessment from the government of San Bernardino County, California as a demonstration
        - Purpose is to validate compliance with specific regulations and minimize

cybersecurity risks

- Preparing for a HIPAA External Assessment
  - Examiners provide a checklist of questions that organizations must answer
  - Questions are answered as either "yes" or "no"
  - Evidence files, such as documents or links, must be provided to demonstrate compliance
- Sample Checklist
  - Questions cover various aspects like general information, policies, procedures, and employee training
  - Organizations must provide evidence files as proof of compliance
  - External assessments aim to provide a quick overview of the organization's current risk posture

- **Penetration Testing**
  - *Penetration Testing (Pentesting)*
    - Simulated cyber attack to identify exploitable vulnerabilities in a computer system
    - Assesses systems for potential weaknesses that attackers could exploit
    - Various types include
      - Physical
      - Offensive
      - Defensive
      - Integrated

- *Physical Penetration Testing*
  - Evaluates an organization's physical security measures
  - Examples
    - Testing locks
    - Access card
    - Security cameras
  - Identifies vulnerabilities and recommends improvements for enhanced physical security
  - Benefits
    - Improved security awareness
    - Preventing unauthorized access
- *Offensive Penetration Testing*
  - Known as “red teaming”
  - Actively seeks vulnerabilities and attempts to exploit them, like a real cyber attack
  - Helps uncover and report vulnerabilities to improve security
  - Can simulate real-world attacks and gain support for cybersecurity investments
- *Defensive Penetration Testing*
  - Known as “blue teaming”
  - A reactive approach focused on strengthening systems, detecting and responding to attacks
  - Monitors for unusual activity and improves incident response times
  - Enhances detection capabilities and helps improve incident response
- *Integrated Penetration Testing*
  - Known as “purple teaming”
  - Combines elements of offensive and defensive testing

- Red team conducts offensive attacks, while the blue team detects and responds
- Encourages collaboration and learning between the red and blue teams
- Benefits
  - Comprehensive security assessment
  - Promotes collaboration within cybersecurity teams
  - Conducts simulated attacks and responses to improve skills

- **Reconnaissance in Pentesting**
  - *Reconnaissance*
    - Initial phase where an attacker gathers information about the target system
    - Information helps plan the attack and increase its success rate
  - Importance of Reconnaissance
    - Crucial step in penetration testing
    - Identifies potential vulnerabilities in the target system
    - Helps plan the attack to reduce the risk of detection and failure
  - Types of Reconnaissance
    - *Active Reconnaissance*
      - Engaging with the target system directly, such as scanning for open ports using tools like Nmap
    - *Passive Reconnaissance*
      - Gathering information without direct engagement, like using open-source intelligence or WHOIS to collect data
  - Reconnaissance and Environment Types
    - *Known Environment*
      - Penetration testers have detailed information about the target

infrastructure

- Focuses on known assets
- Evaluates vulnerabilities and weaknesses
- Aims to understand exploitability and potential damages
- Resembles an insider threat scenario

- *Partially Known Environment*
  - Testers have limited information, simulating a scenario where an attacker has partial inside knowledge
  - Focus on discovering and navigating the broader environment
- *Unknown Environment*
  - Minimal to no information about the target system
  - Simulates a real-world external attacker aiming to find entry points and vulnerabilities
  - Extensive reconnaissance is essential

- **Performing a Basic PenTest**
  - *Metasploit*
    - Multipurpose computer security and penetration testing framework
    - Has a wide array of powerful tools for conducting penetration tests

- **Attestation of Findings**
  - *Attestation*
    - Involves formal validation or confirmation provided by an entity to assert the accuracy and authenticity of specific information
    - Crucial in internal and external audits to ensure the reliability and integrity of the following

        - Data
        - Systems
        - Processes
    - Attestation of Findings in Penetration Testing
        - Used to prove that a penetration test occurred and validate the findings
        - May be required for compliance or regulatory purposes (e.g., GLBA, HIPAA, Sarbanes-Oxley, PCI DSS)
        - Includes a summary of findings and evidence of the security assessment
        - Evidence helps to prove that identified vulnerabilities and exploits are valid
        - The difference between attestation and the report
            - Attestation includes evidence
            - Report focuses on findings and recommended remediation
        - A letter of attestation may be provided to prove the occurrence of the penetration testing, especially when required by third parties interested in network security
    - Types of Attestation
        - *Software Attestation*
            - Involves validating the integrity of software to ensure it hasn't been tampered with
        - *Hardware Attestation*
            - Validates the integrity of hardware components to confirm they haven't been tampered with
        - *System Attestation*
            - Validates the security posture of a system, often related to compliance with security standards

- Attestation in Audits
  - In internal audits, attestation evaluates organizational compliance, effectiveness of internal controls, and adherence to policies and procedures
  - In external audits, third-party entities provide attestation on financial statements, regulatory compliance, and operational efficiency
  - Attestation builds trust, enhances transparency, ensures accountability, and is essential for stakeholders in making informed decisions