

CompTIA Security+ (SY0-701) Day 8

Section 5.2: Explain the Elements of the Risk Management Process

Risk - An undeterminable future event resulting from a given action, activity, or inaction.

- Often seen as the potential for harm or loss in terms of personnel, reputation, assets, financial stability, or the ability to successfully execute strategies.

Risk Identification Methods

- **Brainstorming** - A group discussion technique where stakeholders generate as many potential risks as possible without immediate judgment or evaluation.
- **Checklist** - Using pre-defined lists of common risks or controls to ensure nothing is overlooked during risk identification.
- **Historical Information** - Reviewing past incidents, audits, or lessons learned to identify risks that have occurred before or could occur again.
- **SWOT Analysis** - A structured approach to evaluating **Strengths, Weaknesses, Opportunities, and Threats** to identify internal and external risks.
- **Researching** - Gathering information from industry reports, white papers, threat intelligence feeds, and best practices to identify potential risks.
- **Interview and Self-Assessments** - Collecting input from staff, management, or third parties to uncover risks from multiple perspectives.
- **Expert Consultation** - Leveraging the knowledge and experience of subject matter experts to identify potential risks and vulnerabilities.
- **Technological Tools** - Using automated tools (e.g., vulnerability scanners, SIEMs) to identify risks and weaknesses in systems and processes.

Risk Assessment

- Evaluating the potential risk that was identified during risk identification.
 - **Probability or Likelihood**
 - **Impact or Consequence**

Elements of a Risk Assessment

- **Risk Estimation** - Determining the likelihood and potential impact of each identified risk, either quantitatively or qualitatively.
- **Risk Evaluation** - Comparing estimated risks against established criteria such as risk appetite or regulatory requirements to determine their significance.
- **Risk Prioritization** - Ranking risks based on their severity to ensure the most critical risks are addressed first.
- **Risk Documentation** - Recording identified risks, their assessments, and treatment plans in a structured format (e.g., risk register).

Types of Risk Assessment

- **Ad Hoc** - Performed as needed, in response to a specific event, change in environment, or when new information becomes available. Reactive in nature.
- **Recurring** - Conducted at regular intervals as part of a structured risk management program. Ensures ongoing monitoring and updates to the risk landscape.
- **One-Time** - Performed for a particular project, process, or system implementation. Specific to a point in time.
- **Continuous** - Integrated into operations, relying on real-time data and tools to provide ongoing insights and immediate responses to emerging risks.

Qualitative Risk Management

- Uses subjective judgment and expert opinion.
- Does not attempt to assign absolute numeric values. Focuses on: likelihood and impact.
- Useful when numerical data is difficult to obtain.
- Employs categories like **High, Medium, Low** for severity and likelihood.
- Guides risk decisions: **Avoid, Transfer, Mitigate, Accept**.

Defining Likelihood

- **Low** - 0–25% chance of threat occurring in one year.
- **Moderate** - 26–75% chance of threat occurring in one year.
- **High** - 76–100% chance of threat occurring in one year.

Impact

- The effect on the organization from a **CIA (Confidentiality, Integrity, Availability)** standpoint if the risk occurs.
- Impact and likelihood combine to produce a risk rating.

Quantitative Risk Analysis

- Focuses on numerical and monetary values.
- **Asset Value (AV)** - Monetary value of the asset.
- **Exposure Factor (EF)** - Percentage of loss expected from a specific threat.
- **Single Loss Expectancy (SLE)** - Monetary loss for each occurrence of a threat.
 - Formula: $SLE = AV \times EF$
- **Annualized Rate of Occurrence (ARO)** - Estimated frequency of a threat occurring in a year.
- **Annualized Loss Expectancy (ALE)** - Expected monetary loss for an asset due to a particular risk over one year.
 - Formula: $ALE = SLE \times ARO$

Risk Register

- A document used for analyzing risks and driving action to:
 - Reduce likelihood of risks.
 - Increase visibility of risks.
 - Improve ability to handle risks if they occur.
 - Reduce impact of risks.

Key Components:

- **Key Risk Indicators** - Metrics signaling increasing or decreasing exposure.
- **Risk Owners** - Individuals accountable for managing a risk.
- **Risk Threshold** - Level of risk exposure above which risks are not acceptable.

Risk Appetite

- Defines the types of risk an organization is willing to accept in pursuit of objectives.

Types:

- **Expansionary** - Willing to accept higher risk for rapid growth or advantage.
- **Conservative** - Risk-averse, focusing on stability.
- **Neutral** - Balanced, accepting calculated risks aligned with objectives.

Risk Tolerance

- Quantifies the amount of risk an organization is willing to accept.
- More specific than risk appetite.
- Often measurable and tied to certain activities or departments.
- Guides budget, resource planning, and strategic decisions.

Risk Management Strategies

- **Avoid** - Prevent the exploitation of a vulnerability.
- **Transfer** - Shift the risk to another party (e.g., insurance, outsourcing).
- **Mitigate** - Reduce damage through planning and controls.
- **Accept** - Do nothing and accept the loss if it occurs.

Business Impact Analysis (BIA)

- Assesses potential effects of interruptions to critical operations.
- Examples of impacts: Loss of sales, production delays, increased expenses, reputational damage.

BIA Concepts:

- **Recovery Time Objective (RTO)** - Target time for resuming operations.
- **Recovery Point Objective (RPO)** - Maximum acceptable data loss.
- **Mean Time to Repair (MTTR)** - Average repair time for a failure.
- **Mean Time Between Failures (MTBF)** - Average time between repairable failures.

Section 5.3: Explain the Processes Associated with Third-Party Risk Assessment and Management

Vendor Selection

- **Due Diligence:** Detailed background checks and research on potential vendors.
 - **Financial stability:** Examine balance sheets, profit-loss statements, and credit ratings.
 - **Reputation:** Research reviews, customer testimonials, and any negative press.
- **Conflict of Interest:** Ensuring impartiality and ethical business conduct.
 - **Relationship Disclosure:** Both parties should disclose any relationships that could affect the contract.
 - **Ethical Guidelines:** Set expectations for avoiding conflicts of interest, such as prohibiting gifts that could sway decisions.
- **Vendor Assessment**
 - **Penetration Testing:** Evaluating the vendor system for vulnerabilities.
 - **Right-to-Audit Clause:** The right to audit the vendor's compliance.
 - **Evidence of Internal Audits:** Documented proof of internal audit results.
 - **Independent Assessments:** Third-party evaluation of the vendor's security.
 - **Supply Chain Analysis:** Assessment of risk in the vendor's supply chain.

Agreement Types

- **Service Level Agreement (SLA)** - A formal contract that defines the level of service expected from a vendor, including uptime, performance benchmarks, and responsibilities of both parties.
- **Memorandum of Agreement (MOA)** - A document that outlines the terms and details of a cooperative agreement between parties, including roles and responsibilities.
- **Memorandum of Understanding (MOU)** - A non-binding agreement between parties that indicates an intended common line of action or partnership.
- **Master Service Agreement (MSA)** - A contract that establishes the overall terms and conditions between parties for future transactions or work. It streamlines negotiations by setting standard terms so that only project-specific details need to be defined in later agreements (e.g., SOWs).
- **Statement of Work (SOW) / Work Order (WO)** - A formal document that defines project-specific activities, deliverables, timelines, and responsibilities agreed upon by both parties.

- **Non-Disclosure Agreement (NDA)** - A legally binding contract that establishes confidentiality between parties and restricts the sharing of sensitive information.
- **Business Partner Agreement (BPA)** - A formal contract that defines the roles, responsibilities, and obligations of business partners, often used to ensure proper handling of sensitive data in compliance with regulations (e.g., HIPAA in healthcare).

Vendor Monitoring

- Ensures throughout the duration of their relationship with an organization:
 - Vendors comply with contractual agreements
 - Continue to meet performance and security standards

Questionnaires - Collect detailed information about vendors' practices, policies, and controls.

- To evaluate the risk associated with a potential or current vendor relationship:
 - **Frequency** - Determine how often questionnaires should be sent
 - **Focus Areas** - Tailor questions to assess key risk areas such as security, quality, and performance.
 - **Tracking** - Maintain a record of past questionnaire responses for trend analysis.

Rules of Engagement

- Agreed-upon terms, conditions, and protocols that dictate how third-party interactions will occur.
 - Especially regarding security and compliance matters.
 - Ensures that interactions with third parties do not pose undue risk to an organization.

Section 5.4: Summarize Elements of Effective Security Compliance

Security Compliance

- The process of **adhering** to established laws, regulations, standards, and policies that govern the protection of information and information systems.

Compliance Reporting

- The process of **documenting and submitting evidence** to demonstrate that an organization is adhering to relevant laws, regulations, standards, and internal policies.

Consequences of Non-compliance

- **Fines:** Monetary penalties for violations.
- **Sanctions:** Restricted business operations.
- **Reputational Damage:** Negative impact on brand.
- **Loss of License:** Revoking the right to operate.
- **Contractual Impacts:** Legal consequences, possibly leading to termination of contracts.

Compliance Monitoring

- The ongoing process of reviewing and evaluating an organization's adherence to relevant laws, regulations, and internal policies.
 - **Due Diligence/Care:** Proactively ensuring compliance through audits and checks.
 - **Attestation and Acknowledgment:** Verifying and documenting compliance.
 - **Internal and External:** Compliance oversight both within and outside the organization.
 - **Automation:** Utilizing software tools for ongoing compliance tracking.

Privacy

- **Why Privacy Breaches Are Concerning**
 - Consequences of breaches can be severe:
 - Damage to reputation, Loss of business, Legal fines, Identity theft, Loss of intellectual property, and Exposure to lawsuits.
 - Many jurisdictions have passed mandatory reporting regulations - have a plan in place!
 - Local, National, Global
- **Data Classification**
 - Data should be classified according to its sensitivity and secured appropriately.
 - Organizations may adopt different classification schemes, but common classification levels include:
 - Private, Public, Confidential, Sensitive, Proprietary, and Critical.
- **Key Elements of Privacy**
 - **Data Subject** - Recognizing and safeguarding the rights of individuals.
 - **Controller vs Processor** - Differentiating roles as they have different obligations and responsibilities under privacy laws.
 - **Ownership** - Individuals retain ownership over their personal data.
 - **Data Inventory and Retention** - Maintaining an inventory of the data collected and retaining it only for its intended purpose.
 - **Right to be Forgotten** - Ensures individuals can request deletion of their personal data.

Section 5.5: Explain Types and Purposes of Audits and Assessments

Audits and Assessments

- Critical tools used to systematically evaluate and verify an organization's compliance with legal, regulatory, and internal standards.

Internal Audits and Assessments - An independent, objective evaluation conducted within an organization.

- Used to assess the effectiveness of its risk management, control, and governance processes.
 - Aims to identify areas of improvement, ensure compliance with laws and internal policies, and help the organization achieve its objectives.
 - **Compliance** - To assess and ensure that the organization's security program aligns with and adheres to relevant laws, regulations, and standards.
 - Involves reviewing security policies, procedures, and practices.
 - **Audit Committee** - Facilitated by the organization's audit committee.
 - Aim to provide oversight and ensure that the security program effectively manages risk and protects organizational assets.
 - Includes reviewing the effectiveness of security controls, incident response plans, and risk management strategies.
 - **Self-Assessments** - Proactively identify and address vulnerabilities and inefficiencies within the security program before they are exposed by external audits or lead to security incidents.
 - Less formal and more frequent, involving staff evaluating their own compliance with security policies and procedures.

External Audits and Assessments - An independent evaluation conducted by an entity outside of the organization.

- Assess adherence to regulatory standards, industry practices, or contractual obligations.
- Aims to provide an unbiased review of the organization's processes and controls to uncover areas of compliance and risk.
 - **Regulatory** - Ensure the organization's compliance with specific government or industry regulations related to information security and data protection.
 - Conducted by regulatory bodies or their authorized representatives, and focused on adherence to legal requirements, standards, and guidelines.

- **Examinations** - Conduct a detailed inspection and analysis of the organization's security measures.
 - Often in response to specific incidents or as part of routine regulatory oversight.
 - More focused and in-depth than general audits.
 - Assess the effectiveness of the security controls in place.
- **Assessment** - Provide an objective evaluation of the organization's security practices.
 - Often, to meet specific contractual requirements or to gain certifications.
 - Conducted by external consultants or assessors.
 - Offer an unbiased view of the security program's effectiveness, identifying gaps and suggesting improvements.
- **Independent Third-Party Audit** - Provide an impartial and comprehensive review of the organization's security program.
 - Purpose of certification, investor assurance, or partner/vendor requirements.
 - Audits are comprehensive, covering all aspects of the security program.
 - They provide credibility and assurance.

Penetration Testing

Penetration Testing - A simulated cyberattack against a computer system, network, or web application to identify vulnerabilities and security weaknesses.

- Mimics the actions of potential attackers to assess the effectiveness of security and to discover exploitable flaws.

Physical Penetration Testing

- **Purpose:** To test the physical security measures of an organization, like locks, alarms, security personnel, and access control systems.
- **Perspective:** Focuses on identifying vulnerabilities in physical barriers and procedures that protect critical assets.

Offensive Penetration Testing (Red Team)

- **Purpose:** To actively exploit vulnerabilities in systems, networks, or applications, simulating an attacker's perspective.

- **Perspective:** Emphasizes identifying and exploiting weaknesses to understand the potential impact of a successful breach.

Defensive Penetration Testing (Blue Team)

- **Purpose:** To evaluate the effectiveness of defensive mechanisms, such as firewalls, intrusion detection systems, and incident response procedures.
- **Perspective:** Focuses on testing and improving the organization's ability to detect, respond to, and mitigate attacks.

Integrated Penetration Testing (Purple Team)

- **Purpose:** To conduct a comprehensive assessment that includes both offensive and defensive aspects, along with testing of policies and employee awareness.
- **Perspective:** Provides a holistic view of the security posture, integrating technical, procedural, and human factors.

Known Environment Penetration Testing (White-Box Testing)

- **Purpose:** Conducted in an environment where the test participant has full knowledge of the network and systems.
- **Perspective:** Assess security in a controlled setting where all variables are known, providing a thorough examination of specific aspects.

Unknown Environment Penetration Testing (Black-Box Testing)

- **Purpose:** Performed with no prior knowledge of the target system or network, simulating an external attacker.
- **Perspective:** Evaluates the organization's security posture from the perspective of an uninformed attacker.

Partially Known Environment Penetration Testing (Gray-Box Testing)

- **Purpose:** The tester has limited knowledge of the environment, akin to a real-world scenario where an attacker has some information.
- **Perspective:** Tests the organization's security from a semi-informed attacker's point of view, offering a more realistic assessment.

Reconnaissance Penetration Testing

- **Purpose:** To gather information about a target system, network, or organization to identify vulnerabilities and prepare for more effective penetration testing or cyber attacks.
 - **Passive:** Involves gathering information without directly interacting with the target, reducing detection risk.
 - **Active:** Directly engages with the target system to gather information, which can be more revealing but also riskier in terms of detection.

Section: 5.6: Given a Scenario, Implement Security Awareness Practices

Security Awareness Practices

- Educating and training employees about various **cybersecurity threats**.
- Teaching them how to **recognize and respond** to these threats.
- Developing comprehensive **security policies and procedures**.
- Ensuring all staff are aware of and understand their **roles in relation to security**.

Phishing

- **Campaigns:** Run simulated phishing campaigns to educate employees on how real phishing attempts look and feel.
 - Helps raise awareness and prepare them to identify actual threats.
- **Recognizing a Phishing Attempt:** Train employees to recognize signs such as suspicious email addresses, urgent or threatening language, and unexpected attachments or links.
- **Responding to Reported Suspicious Messages:** Establish a clear protocol for employees to report suspected phishing attempts.
 - Ensure prompt and effective responses by the IT/security team.

Anomalous Behavior Recognition

- **Risky:** Educate employees about behaviors that pose risks, like downloading unknown attachments or using unauthorized software.
- **Unexpected:** Train staff to recognize and report unexpected changes in system performance or user activities, which could indicate a security breach.
- **Unintentional:** Highlight common unintentional behaviors that compromise security, like sharing passwords or leaving devices unattended, and how to avoid them.

User Guidance and Training

- **Policy/Handbooks:** Develop comprehensive security policies and handbooks, and ensure all employees are familiar with them.
- **Situational Awareness:** Train employees to be aware of their surroundings and potential security risks, especially in public or unsecured areas.
- **Insider Threat:** Educate about the signs of insider threats and the importance of reporting suspicious internal activities.
- **Password Management:** Teach best practices for creating and managing strong passwords and using password managers.
- **Removable Media and Cables:** Teach the risks associated with unknown or untrusted removable media and cables, and proper usage policies.
- **Social Engineering:** Train employees to recognize and respond to social engineering tactics (e.g., pretexting, tailgating).
- **Operational Security:** Instruct on best practices for handling sensitive information and enforcing access controls.
- **Hybrid/Remote Work Environments:** Provide specific guidelines and training for securing data and devices in remote or hybrid work settings.

Reporting and Monitoring

- **Initial:** Establish a baseline to record where the organization started.
- **Recurring:** Track progress over time to see whether security awareness is improving or declining.

Development and Execution

- **Development:** Create a comprehensive security awareness program that addresses the specific needs and risks of the organization. This should involve collaboration with different departments to ensure all aspects of security are covered.
- **Execution:** Implement the program through a combination of training sessions, simulations, regular communications, and assessments to ensure ongoing awareness and adherence to security practices.