CompTIA Security+ Exam SY0-701

Lesson 15

Explain Risk Management Processes

Lesson 15

Topic 15A

Risk Management Processes and Concepts

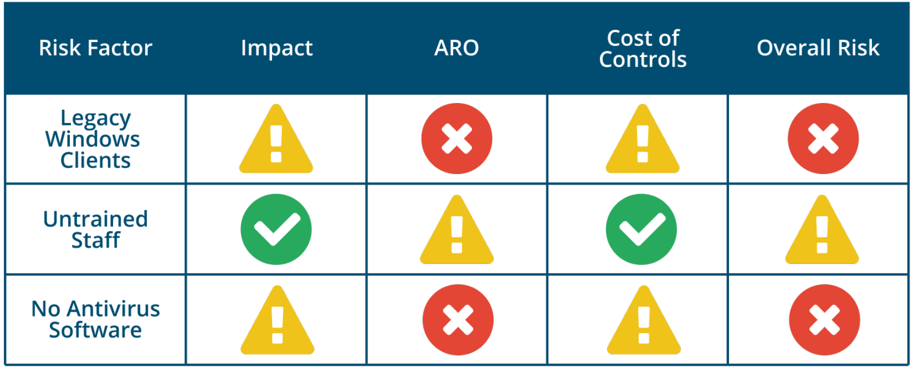
Risk Identification and Assessment (1 of 3)

- Risk identification is fundamental to managing risk
    - Malware attacks
    - Phishing attempts
    - Insider threats
    - Equipment failures
    - Software vulnerabilities
    - Nontechnical risks like inadequate policies or training
- Risk assessment evaluates previously identified risks to determine their potential impact on the organization

Risk Identification and Assessment (2 of 3)

- Risk Analysis
  - Describes identifying and evaluating potential risks and the characteristics that define them
- Quantitative Analysis
  - Assign tangible values to each risk
- Qualitative Analysis
  - Assess risks based on subjective judgment
- Risk Assessment
  - Estimates potential risk levels and their significance by interpreting data collected during risk analysis

Risk Identification and Assessment (3 of 3)



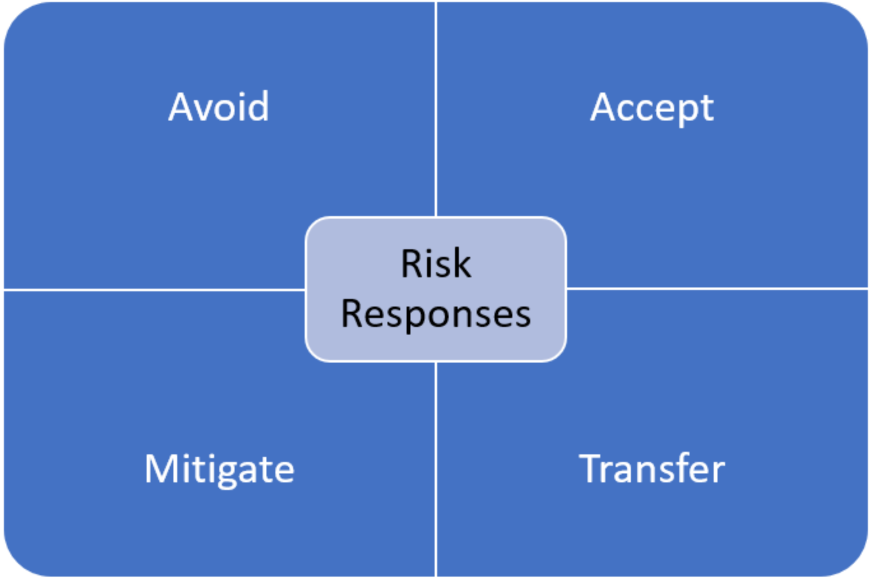
Risk Factor	Impact	ARO	Cost of Controls	Overall Risk
Legacy Windows Clients	⚠	✖	⚠	✖
Untrained Staff	✓	⚠	✓	⚠
No Antivirus Software	⚠	✖	⚠	✖

Traffic light impact grid.

- Inherent Risk
  - Level of risk before any type of mitigation has been attempted
- Heat Map

Risk Management Strategies (1 of 2)

- Risk management strategies
  - Describe the proactive and systematic approaches used to identify, assess, prioritize, and mitigate risks to minimize their negative impacts
- Risk responses
  - Identify how risk items are managed



The four risk responses are avoid, accept, mitigate, and transfer.

Risk Management Strategies (2 of 2)

- Residual Risk
  - The amount of risk left after mitigations are implemented
  - Risk cannot be fully eliminated
- Risk Appetite
  - Acceptable levels of risk
  - Varies from one organization to another
  - Sometimes defined in a formal risk appetite statement

Risk Management Processes (1 of 2)

- Identifying, assessing, and mitigating vulnerabilities and threats to the essential functions that a business must perform to fulfill its purpose
- Risk
  - A measure of threats, vulnerabilities, impact, and probability
- Risk Registers
  - Risk description
  - Severity
  - Owner of the risk item
  - Identified mitigations
  - Often utilize heat maps

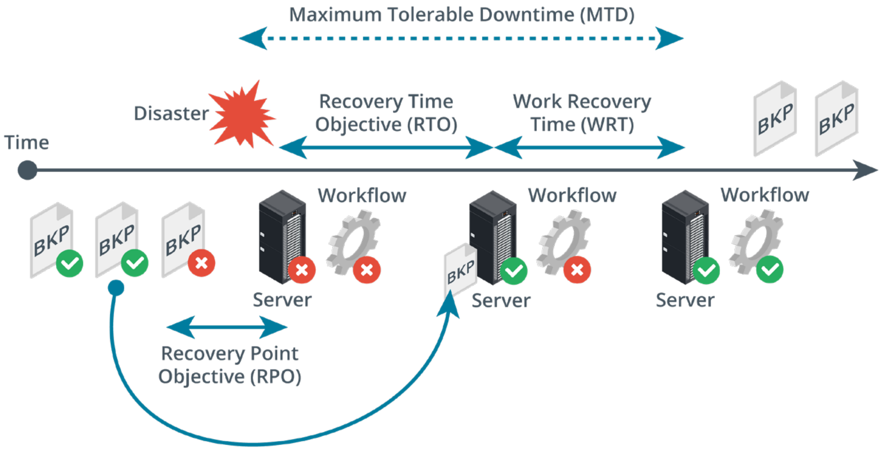
Risk Management Processes (2 of 2)

- Risk Threshold
  - Defines the limits or levels of acceptable risk
- Key Risk Indicators
  - Predictive indicators for monitoring and predicting potential risks
- Risk Reporting
  - Communicate an organization's risk profile
  - Communicate the effectiveness of a risk management program

Business Impact Analysis

- Identification of Critical Systems
- Mission Essential Functions

- Maximum Tolerable Downtime (MTD)
- Recovery Time Objective (RTO)
- Work Recovery Time (WRT)
- Recovery Point Objective (RPO)



Metrics governing mission essential functions. (Images © 123RF.com.)

Review Activity: Risk Management Processes and Concepts

- Risk Identification and Assessment
- Risk Management Strategies
- Risk Management Processes
- Business Impact Analysis

Lesson 15

Topic 15B

Vendor Management Concepts

Vendor Selection (1 of 2)

- Systematically evaluate and assess potential vendors to minimize risks associated with outsourcing or procurement
- Third-Party Vendor Assessment
  - Critical component of Governance, Risk, and Compliance (GRC)
  - Vendor assessments provide evidence of due diligence
- Conflict of Interest
  - When an individual or organization has competing interests or obligations that could compromise their ability to act objectively, impartially, or in the best interest of the organization

Vendor Selection (2 of 2)

- Vendor Assessment Methods
  - Evidence of Internal Audits
  - Independent Assessments
  - Penetration Testing
  - Supply Chain Analysis
  - Right-to-Audit Clause
- Vendor Monitoring
  - Continuously evaluating vendors to ensure ongoing adherence to security standards, compliance requirements, and contractual obligations

Legal Agreements

- Initial Agreements
  - Memorandum of Understanding (MOU)
  - Nondisclosure Agreement (NDA)
  - Memorandum of Agreement (MOA)
  - Business Partnership Agreement (BPA)
  - Master Service Agreement (MSA)
- Operational/Performance Agreements
  - Service-level Agreement (SLA)
  - Statement of Work (SOW)/Work Order (WO)
- Expectations
  - Rules of Engagement (RoE)

Review Activity: Vendor Management Concepts

- Vendor Selection
- Vendor Assessment Methods
- Legal Agreements

Lesson 15

Topic 15C

Audits and Assessments

Attestation and Assessments

- Attestation
  - Verifying the accuracy, reliability, and effectiveness of security controls
- Internal Assessment
  - Organization's own employees conduct an in-depth assessment
  - Relatively simple to perform and customize
- External Assessment
  - Independent Third-Party
  - Impartial and objective evaluation of business practices
  - Required for legal compliance

Penetration Testing

- Uses authorized hacking techniques to discover exploitable weaknesses in the target's security systems.
- Sometimes referred to as Pen Test or Ethical Hacking
- Internal Pen Test performed by a “Red Team”
- May include Active and Passive Reconnaissance
- Known Environment Penetration Testing
- Partially Known Environment Penetration Testing
- Unknown Environment Penetration Testing

Exercise Types

- Different types of penetration tests allow organizations to use a flexible and prioritized approach toward security assessment
- Offensive Penetration Testing “Red Team”
- Defensive Penetration Testing “Blue Team”
- Physical Penetration Testing
- Integrated Penetration Testing
  - Combines different types of penetration testing techniques

Review Activity: Penetration Testing Concepts

- Attestation and Assessments
- Penetration Testing
- Exercise Types

Lab Activity

- Assisted Lab: Performing Reconnaissance
- Assisted Lab: Performing Penetration Testing

CompTIA Security+ Exam SY0-701

Lesson 15

Summary