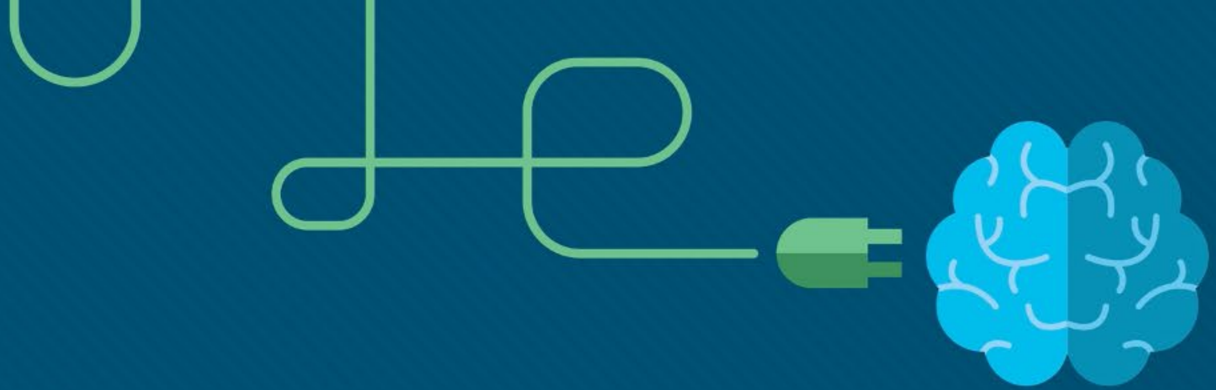


Module 26: Risk Management and Security Controls

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Risk Management and Security Controls

Module Objective: Select security controls based on risk assessment outcomes.

Topic Title	Topic Objective
Risk Management	Explain risk management
Risk Assessment	Calculate risks.
Security Control	Evaluate security controls according to organization characteristics.

26.1 Risk Management

Risk Types

- Risk is the probability of loss due to a threat — a malicious act or unexpected event — that damages information systems or organizational assets.
- Risk impact is the damage incurred by an event which causes loss of asset(s) or disruption of service(s).
- The goal of risk management is to reduce these threats to an acceptable level and to implement controls to maintain that level.
- Threat levels can be classified as:
- **High Risk** - Negligence means that no actions or controls are taken to lower risk. The threat is extremely high, and the cost of an incident could be catastrophic.
- **Lower Risk** - Exercising due care can help lower the level of risk. The risk still exists but these reasonable steps lower a potential loss.
- **Acceptable Risk** - Exercising due diligence involves taking reasonable steps to eliminate risk. Some risks still exist, but multiple controls are implemented to prevent potential loss.

Risk Management

Risk Types (Cont.)

- Risk can be internal, external, or both. Its impact can ripple through the whole organization and affect other external entities.

- Promoting risk awareness within the organization helps employees to develop an understanding of what risks exist, their potential impact and how the organization can manage those risks.

Lab - Risk Management

In this Lab, you will meet the following objectives:

- Part 1: Explain Risk Action Levels
- Part 2: Explain Risk Management Concepts
- Part 3: Explain Risk Management Processes

The Risk Management Process

- Risk management is a formal process that measures the impact of a threat and the cost to implement controls or countermeasures to mitigate that threat.
- Risk cannot be eliminated completely but it can still be managed to an acceptable level.
- All organizations accept some risk, and the cost of a counter measure should **not** be more than the value of the asset being protected.
- The stages of the risk management process include:
  - Frame the Risk
  - Assess the Risk
  - Respond to the Risk
  - Monitor the Risk

The Risk Management Process (Cont.)

Term	Description
Frame the Risk	Identify the threats throughout the organization that increase risk. Threats identified include loss or damage of processes and products, attacks, potential failure or disruption of services, harm to the organization’s reputation, legal liability, and loss of intellectual property.
Assess the Risk	Once a risk has been identified, it is assessed and analyzed to determine the severity that the threat poses. Some threats can bring the entire organization to a standstill while other threats are merely minor inconveniences. Risk can be prioritized by actual financial impact (quantitative analysis) or a scaled impact on the organization's operation (qualitative analysis).
Respond to the Risk	Develop an action plan to reduce overall organization risk exposure. Management ranks and prioritizes threats; a team then determines how to respond to each threat. Risk can be eliminated, mitigated, transferred, or accepted.
Monitor the Risk	Continuously review risk reductions due to elimination, mitigation, and transfer actions. Not all risks can be eliminated, so threats that are accepted need to be closely monitored. An organization can use a risk register — a software program or cloud service — to record information about identified risks. The risk register contains details about the risk and the controls implemented or response strategies used.

26.2 Risk Assessment

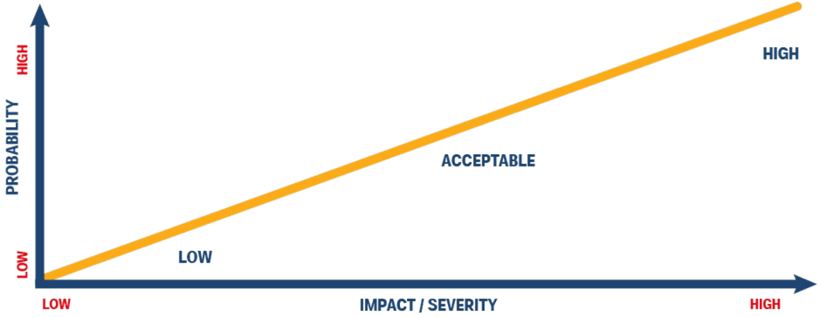
Threat Source Types

- A threat is the potential that a vulnerability will be identified and exploited, while a threat vector is the path that an attacker utilizes to impact the target.

- Threat source types are categorized as follows and can be internal or external.
  - **Adversarial**: Threats from individuals, groups, organizations, or nations.
  - **Accidental**: Actions that occur without a malicious intent.
  - **Structural**: Equipment and software failures.
  - **Environmental**: External disasters that can be either natural or human-caused, such as fires and floods.

Risk Assessment Methodology

- Organizations assess and examine their operational risks by performing a risk assessment to ensure their risk management meets all their business objectives.
- Trying to determine the probability of an attack by a human threat source can be difficult and may involve assessing skill level, motive, opportunity, and size.
- When assessing vulnerability, factors such as ease of discovery, exploitability, awareness, and intrusion detection play a part.
- Use a combination of estimation and historical data to provide the most accurate probability of an event occurring.
- Finally, determine the magnitude of the impact. A simple measure of impact can range from very low to extremely high or from an insignificant impact to a catastrophic impact.



Risk Assessment

Risk Analysis

- Risk analysis examines the dangers posed by natural and human-caused events to the assets of an organization.

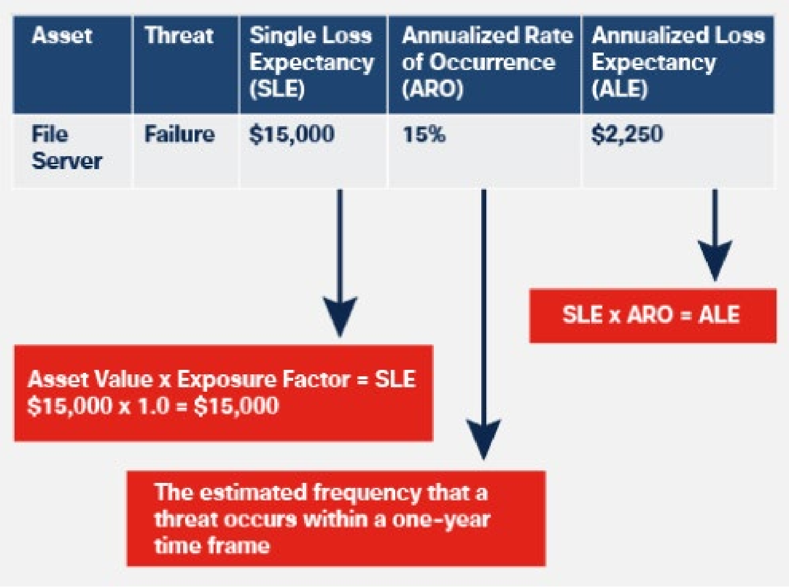
- A user performs an asset identification to help determine which assets to protect.

- A risk analysis has four goals:
  1. Identify assets and their value.
  2. Identify vulnerabilities and threats.
  3. Quantify the probability and impact of the identified threats.
  4. Balance the impact of the threat against the cost of the countermeasure.

- Two approaches to risk analysis are:
  - Quantitative risk analysis
  - Qualitative risk analysis

Risk Analysis (Cont.)

- A quantitative risk analysis assigns numbers to the risk analysis process.
- In this example, the **asset value** is the replacement cost of the file server (the asset).
- The value of an asset can also be measured by the income gained using the asset.
- The **exposure factor (EF)** is a subjective value expressed as a percentage of the file server lost due to a particular threat. If total loss occurs, the EF equals 1.0 (100%).
- The **annualized rate of occurrence (ARO)** is the probability that a loss will occur during the year. An ARO can be greater than 100% if a loss can occur more than once a year.
- The calculation of the **annual loss expectancy (ALE)** gives management some guidance on what an organization should spend to protect the file server.



Asset	Threat	Single Loss Expectancy (SLE)	Annualized Rate of Occurrence (ARO)	Annualized Loss Expectancy (ALE)
File Server	Failure	$15,000	15%	$2,250

SLE x ARO = ALE

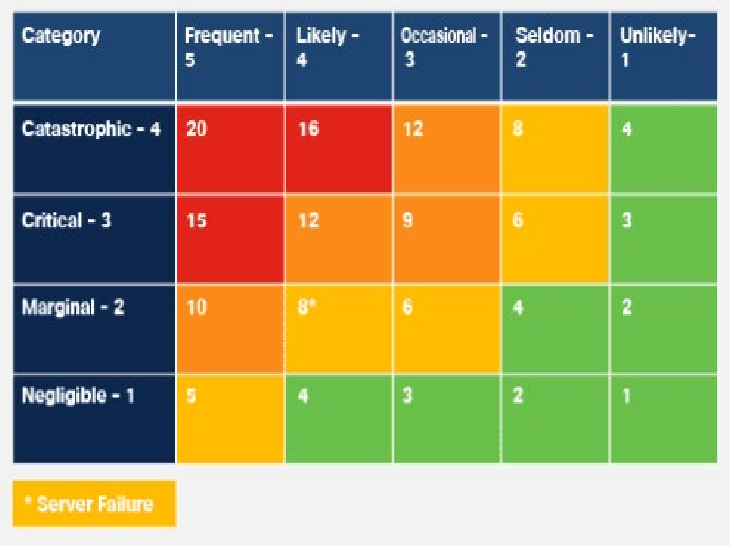
Asset Value x Exposure Factor = SLE
$15,000 x 1.0 = $15,000

The estimated frequency that a threat occurs within a one-year time frame

Risk Analysis (Cont.)

Qualitative risk analysis

- Qualitative risk analysis uses opinions and scenarios plotting the likelihood of a threat against its impact.
- For example, a server failure may be likely, but its impact may only be marginal.
- A risk matrix is a tool that helps prioritize risks to determine which ones the organization needs to develop a response for.
- The results can be ranked and used as a guide to determine whether the organization takes any action.
- When the risk matrix is color-coded, as shown here, it is referred to as a risk heat map.



Category	Frequent - 5	Likely - 4	Occasional - 3	Seldom - 2	Unlikely- 1
Catastrophic - 4	20	16	12	8	4
Critical - 3	15	12	9	6	3
Marginal - 2	10	8*	6	4	2
Negligible - 1	5	4	3	2	1

* Server Failure

Lab - Risk Analysis

In this Lab, you will meet the following objectives:

- Part 1: Use Risk Analysis Methods
- Part 2: Calculate Risks

Risk Mitigation

- Mitigation involves reducing the likelihood or severity of a loss from threats.
- Many technical controls mitigate risk, including authentication systems, file permissions and firewalls.
- Organizations must understand that risk mitigation can have both positive and negative impacts on the organization.
- Good risk mitigation finds a balance between the negative impact of countermeasures and controls and the benefit of risk reduction.

Risk Mitigation (Cont.)

Most common ways to mitigate against risk are:

Term	Description
Accept the risk and periodically reassess	A short-term strategy is to accept the risk necessitating the creation of contingency plans for that risk. People and organizations must accept risk on a daily basis.
Reduce the risk by implementing controls	Modern methodologies reduce risk by developing software incrementally, and by providing regular updates and patches to address vulnerabilities and misconfigurations.
Avoid the risk by totally changing the approach	A good risk mitigation plan can include two or more strategies.
Transfer the risk to a third party	Outsourcing services, purchasing insurance, and purchasing maintenance contracts are all examples of risk transfer. Hiring specialists to perform critical tasks to reduce risk can be a good decision and yield greater results with less long-term investment.

26.3 Security Controls

Control Types

- The inherent risk of a system is the risk that the system poses inherently — without any people, process, or technology controls in place.

- Security controls are safeguards or countermeasures that an organization implements to avoid, detect, counteract, or minimize security risks to organizational assets.

- The three control types are:

  - **Administrative controls** - consist of procedures and policies that an organization puts into place when dealing with sensitive information. These controls determine how people act.
  - **Technical controls** - involve hardware and/or software implemented to manage risk and provide protection.
  - **Physical controls** - mechanisms such as fences, and locks deployed to protect systems, facilities, personnel, and resources. Physical controls physically separate people or other threats from systems.

Functional Security Controls

The functional use of a specific safeguard or counter measure will help determine the reason for choosing and implementing it.

Term	Description
Preventive controls	Preventive security controls stop unwanted and unauthorized activity from happening and/or apply restrictions for authorized users.
Deterrent controls	A deterrent aims to discourage something from happening.
Detective controls	Access control detection identifies several types of unauthorized activity. They are not a preventive measure and instead focus on the discovery of a security breach after it has occurred.
Corrective controls	They counteract something undesirable by restoring the system back to a state of confidentiality, integrity, and availability. They can also restore systems to normal after unauthorized activity occurs.
Recovery controls	Recovery security controls restore resources, functions, and capabilities back to a normal state after a violation of a security policy.
Comprehensive controls	They provide options to other controls to bolster enforcement in support of a security policy. A compensative control can also be a substitution used in place of a control that is not possible under the circumstances.

Controls and Compliance

- The Center for Internet Security (CIS) has created a mapping of its eighteen critical security controls to some of the common compliance frameworks.
- This provides helpful guidance to security professionals who are working to create and maintain compliance with the required frameworks.
- A Google search on **site: cisecurity.org mapping and compliance** returns a page in which the CIS provides guidance regarding security controls that are relevant to essential industry compliance frameworks such as PCI DSS, the NIST Cybersecurity Framework, FISMA, HIPAA, GDPR, and ISO/IEC 27001.
- Useful links and references are provided to illustrate how the CIS controls enable compliance with the different frameworks.
- In addition, members of the CIS gain access to the CIS-CAT Pro controls guidance and assessment tool that provides assistance in assessing compliance through the mappings of the CIS controls to the individual compliance frameworks.

Lab - Security Controls Implementation

In this lab, you will complete the following objectives:

- Part 1: Review security controls
- Part 2: Complete a security controls grid

26.4 Risk Management and Security ControlsSummary

What Did I Learn in this Module?

- Risk is the probability of loss due to a threat, a malicious act, or an unexpected event that damages information systems or organizational assets.
- Risk impact is the damage incurred by an event which causes loss of asset(s) or disruption of service(s).
- The goal of risk management is to reduce these threats to an acceptable level and to implement controls to maintain that level. Risk can be internal, external, or both.
- The process of risk management requires to frame the risk, assess the risk, and respond to the risk.
- Threat assessment is the foundation for risk assessment.
- A threat is the potential that a vulnerability will be identified and exploited.
- A threat vector is the path that an attacker utilizes to impact the target.
- Threat source types are categorized as adversarial, accidental, structural, and environmental.
- Organizations assess and examine their operational risks by performing a risk assessment to ensure their risk management meets all their business objectives.
- They determine if the threat is low, acceptable, or high.
- A quantitative risk analysis assigns numbers to the risk analysis process.
- A qualitative risk analysis uses opinions and scenarios plotting the likelihood of a threat against its impact.

Risk Management and Security Controls Summary

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

- A risk matrix is a tool that helps prioritize risks to determine which ones the organization needs to develop a response for.
- Several approaches may be considered including accepting the risk and periodically reassessing, reducing the risk by implementing controls, avoiding the risk totally by changing the approach, and transferring the risk to a third party.
- Security controls are safeguards or countermeasures that an organization implements to avoid, detect, counteract, or minimize security risks to organizational assets.
- Administrative controls consist of procedures and policies that an organization puts into place when dealing with sensitive information.
- Technical controls involve hardware and/or software implemented to manage risk and provide protection.
- Physical controls are mechanisms such as fences, and locks deployed to protect systems, facilities, personnel, and resources.
- Functional security controls include preventive, deterrent, detective, corrective, recovery, and compensative controls.