3.2.3 Risk Management Facts

Risk management is the process of identifying vulnerabilities and threats and then deciding which countermeasures will reduce those risks to an acceptable level. The main objective is to reduce an organization's risk to a level that is deemed acceptable by senior management.

To help you better perform a risk analysis, familiarize yourself with the following terms:

Risk Concept	Definition
Asset	An *asset* is a resource that has value to an organization. Assets come in many forms, some of which are: ▪ Information assets, such as files or databases that contain valuable information. ▪ Infrastructure assets or physical devices, such as routers, firewalls, bridges, and servers. ▪ Support services for the information services.
Threat Vector	A *threat vector* is a path or means that an attacker can use to compromise the security of a system. Threat vectors expose a system's vulnerabilities, allowing an attacker to exploit them. Common threat vectors include: ▪ Email attachments ▪ Web pages with embedded scripts ▪ Browser pop-ups ▪ Social manipulation ▪ Poor programming practices ▪ Unpatched operating systems and applications ▪ Outdated security mechanisms and encryption ▪ Breached physical security ▪ Unused applications and services on a system ▪ Enabled USB ports
Threat Probability	*Threat probability* is the likelihood that a particular threat will occur that exploits a specific vulnerability.
Countermeasure	A *countermeasure* is a means of mitigating the potential risk. Countermeasures reduce the risk of a threat agent being able to exploit a vulnerability.
Exposure	*Exposure* is the vulnerability to losses from a threat agent.
Loss	A *loss* is the real damage to an asset that reduces its confidentiality, integrity, or availability.
Risk	*Risk* is the likelihood of a vulnerability being exploited. Reducing the vulnerability or minimizing the threat agent reduces the risk.
Residual risk	*Residual risk* is the portion of risk that remains after the implementation of a countermeasure. Residual risk almost always occurs.

Risk management consists of the following processes:

Process	Description
Asset Identification	Asset identification includes the following processes: ▪ *Asset identification* identifies the organization's resources. ▪ *Asset valuation* determines the worth of that resource to the organization. Asset valuation is important because it establishes the level of protection appropriate for each asset. When identifying assets and values, be sure to include both *tangible* and *intangible* assets. ▪ A *tangible asset* is a physical item such as a computer, storage device, or document. Such items are typically purchased. The valuation of these assets can be easily determined by the cost of replacing the item. ▪ An *intangible asset* is a resource that has value and may be saleable even though it is not physical or material. Intangible assets are typically more challenging to identify and evaluate. Assets can have both tangible and intangible components. For example, a computer that functions as a server has a tangible value associated with the replacement cost of the hardware. Intangible assets include the data on the computer, the value of the role that the computer performs within the organization, and what the computer's information is worth to a competitor or an attacker.
Threat Identification	When identifying threats, consider the various sources of threats: ▪ *External* threats are those events originating outside of the organization that typically focus on compromising the organization's information assets. Examples are hackers, fraud perpetrators, and viruses.

	▪ *Internal* threats are intentional or accidental acts by employees, including:
	  ▪ Malicious acts such as theft, fraud, or sabotage
	  ▪ Intentional or unintentional actions that destroy or alter data
	  ▪ Disclosing sensitive information through snooping or espionage
	▪ *Natural events* are those events that may reasonably be expected to occur over time. Examples are a fire or a broken water pipe.
	▪ *Disasters* are major events that have significant impact on an organization. Disasters can disrupt production, damage assets, and compromise security. Examples of disasters are tornadoes, hurricanes, and floods.

Vulnerability Evaluation	After identifying possible sources of threats, the next step is to evaluate common vulnerabilities to identify weaknesses that can be exploited. Vulnerabilities include: ▪ Software, operating system, and hardware vulnerabilities ▪ Lax physical security ▪ Weak policies and procedures, such as a poor password policy As you identify threats and evaluate vulnerabilities, consider risks that can occur at any point in your company's *supply chain*. The chain typically includes supplying raw materials, manufacturing products, and selling and distributing the products to end customers.
Risk Assessment	Risk assessment is the practice of determining which threats identified are relevant and pressing to the organization and then attaching a potential cost that can be expected if the identified threat occurs. There are two general risk assessment methods: ▪ *Quantitative* analysis assigns real numbers to the costs of damages and countermeasures. It also assigns concrete probability percentages to risk occurrence. ▪ *Qualitative* analysis uses scenarios to identify risks and responses. Qualitative risk analysis is more speculative (based on opinion) and results in relative costs or rankings. Strict quantitative value of the loss is typically not possible. Determination of value must also include qualitative components. Measuring risks quantitatively requires identifying the following components: ▪ *Single loss expectancy* (SLE) is the amount of loss expected for any single successful threat attack on any given asset. This is a monetary value that describes how much the incident will cost in terms of lost asset value. ▪ *Exposure factor* is the percentage of the asset lost because of a successful threat attack. ▪ *Annualized rate of occurrence* (ARO) identifies how often in a single year the successful threat attack will occur. ARO information is frequently obtained from insurance companies, law enforcement agencies, and computer incident monitoring organizations. For example, an ARO of 2 indicates that the incident is expected to occur twice a year, while an ARO of .25 means the incident is expected once every four years. ▪ *Annual loss expectancy* (ALE) estimates the annual loss resulting from an incident. For example, if you expect a successful attack every four years, the ALE for the incident would be 1/4 of the SLE. The quantitative value of risk can be determined with the following calculation: SLE x ARO = ALE. This tells you how much a potential threat costs each year. For example, if the asset loses $1,000 for each incident and you expect an incident every four years, the annual cost for that asset would be $250. As you attempt to quantify and assess risks, consider creating a *risk register* early in the risk management process. A risk register provides details of each known risk, including a risk category, description, unique identification number, projected impact, likelihood of occurring, and risk response plan. This information can be used to create a scatter plot that represents the possible impact of each risk in relation to its overall probability. Having a visual representation of risks can help stakeholders better assess them.

Risk Response	After you have identified the risks and their associated costs, you can determine how best to respond to the risk. Responses include:
	▪ Taking measures to *reduce* (or *mitigate*) the likelihood of the threat by deploying security controls or other protections. When deploying countermeasures, the annual cost of the countermeasures should not exceed the ALE. If it does, you are paying more to protect the asset than it is worth. Security control types include:
	  ▪ Management
	  ▪ Operational
	  ▪ Technical
	Consider the following factors when implementing security controls to reduce risk:
	  ▪ Compatibility with the existing infrastructure
	  ▪ Effectiveness

- Regulatory compliance
- Organizational policies
- Operational (performance) impact
- Feasibility (technical requirements or usability)
- Safety and reliability

- *Transferring* (or *assigning*) risk by purchasing insurance to protect the asset. When the incident occurs, the cost of replacing or reparing the asset is covered by insurance. When deciding to transfer the risk, be sure to compare the cost of insurance with the ALE. Purchase the insurance only if its cost is less than the ALE.
- *Accepting* the risk and choosing to do nothing. For example, you might decide that the cost associated with a threat is acceptable or that the cost of protecting the asset from the threat is unacceptable. In this case, you would plan for how to recover from the threat, but not implement any measures to avoid it.
- *Risk rejection* (or *denial*) is choosing not to respond to the risk even though the risk is not at an acceptable level. Risk rejection introduces the possibility of negligence and may lead to liability. Risk rejection is not an appropriate response.
- *Risk deterrence* is letting threat agents know of the consequences they face if they choose to attack the asset. This could include posting warnings on login pages to indicate prosecution policies.
- *Distributive Allocation* responds to the risk by spreading it through redundancy and high availability techniques such as clustering, load balancing, and redundant storage arrays.

It is not possible to eliminate all risk. Taking actions reduces risk to acceptable levels. Risk that remains after reducing or transferring risk is called *residual* risk.

One goal of asset identification and valuation is to prioritize assets based on the seriousness of potential threats and the impact that a loss would have on normal operations. As you plan protection strategies and allocate security resources and budgeting, start with the most critical assets first. The following table lists several methods you can use to prioritize assets.

Method	Description
Delphi	The *delphi* method uses an anonymous survey to determine the value of an asset. Anonymity promotes honest responses.
Sensitivity vs. Risk	A *sensitivity vs. risk* chart uses quadrants to qualify the value of an asset based on sensitivity and risk. The chart can be used to quantify the value when: ▪ Categories are designated with assigned quantitative value. ▪ Budget amounts are specified for each category. ▪ A numerical ranking compatible with industry valuations is used (this step is optional, but helpful).
Comparative	A *comparative* valuation uses a ranking based on an arbitrary scale that is compatible with the organization's industry. The valuation is still qualitative, but consistency in valuation with other organizations in the industry adds credibility.
Asset Classification	*Asset classification* is used to identify the appropriate value and protection levels. Asset classification can expedite the valuation process by grouping similar assets and comparing the valuation of different classifications. Asset classification: ▪ Is based on the value of the assets and the duration the value is maintained. ▪ Includes a judgment about the sensitivity of the asset. ▪ May be driven by legal and regulatory compliance requirements. ▪ Affects the storage and access controls required to protect the asset. The implementation of classification labels and guidelines for handling labeled information increases the awareness for data protection and provides rules for protecting the data.

Once assets have been identified and a valuation established, it is important to document procedures relating to these classifications and other security procedures. This documentation provides a guideline for what is to be protected and the following how-tos:

- How to store the asset
- How to provide access to the asset
- How to transfer and move the asset
- How to destroy or dispose of the asset