12.2.2 Risk Management Facts

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

Risk Management Terminology

Be familiar with the following terms related to risk analysis:

Risk Concept	Definition
Asset	An *asset* is a resource that has value to the organization. Assets come in many forms. ▪ 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	*Threat* is any potential danger to the confidentiality, integrity, or availability of information or systems.
Vulnerability	*Vulnerability* is the possibility of an asset being exploited due to the absence or weakness of an asset safeguard.
Threat Agent	A *threat agent* is an entity that may find and exploit a vulnerability, causing a threat to an asset.
Threat Vector	A *threat vector* is the path or means that an attacker uses to compromise a system. Threat vectors expose a system's vulnerabilities and are exploited by an attacker. Some 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 methods ▪ Breached physical security ▪ Unused applications and services on a system ▪ Enabled USB ports Due to their nature, portable storage devices pose the greatest threat to confidential data. Organizations that handle highly sensitive data should consider disabling the USB ports on all workstations.
Threat Probability	*Threat probability* is the likelihood that a particular threat will exploit a specific vulnerability of a system.
Attack	An *attack* is an action that intends to compromise an asset by exploiting a vulnerability.
Countermeasure	A *countermeasure* is something done to reduce the likelihood of a successful attack. An appropriate countermeasure should: ▪ Provide a security solution to an identified problem. ▪ Not depend on secrecy. ▪ Be testable and verifiable. ▪ Provide uniform or consistent protection for all assets and users. ▪ Be independent of other safeguards. ▪ Require minimal human intervention. ▪ Be tamper-proof. ▪ Have overrides and fail-safe defaults.
Exposure	*Exposure* is the vulnerability of losses from a threat agent.
Loss	*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

	exists.

Risk Management Process

Risk management consists of the following:

Process	Description
Asset Identification	*Asset identification* establishes the organization's resources. *Asset valuation* determines the worth of each resource to the organization, as well as the level of protection appropriate for each asset. When identifying assets and values, be sure to include both types of assets. ▪ A *tangible asset* is a physical item, such as a computer, storage device, or document. These items are usually purchased, and their values can easily be determined by the cost of replacing them. ▪ 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 difficult to identify and value. 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 importance of the role that the computer performs within the organization, and the value of the computer's information to a competitor or attacker.

Threat Identification	When identifying threats, consider the various sources of threats:
	▪ *External* threats are events originating outside of the organization that compromise the organization's assets. Examples include hackers, fraud perpetrators, and viruses.
	▪ *Internal* threats are intentional or accidental acts by employees, including:
	  ▪ Malicious acts, such as theft, fraud, or sabotage
	  ▪ Actions that destroy or alter data
	  ▪ Disclosure of sensitive information through snooping or espionage
	▪ *Natural events* are events that can be expected to occur over time (e.g., 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/or compromise security. Examples of disasters are tornadoes, hurricanes, and floods.
	In addition to identifying sources of threats, consider common vulnerabilities that can be exploited:
	▪ Software, operating system, and hardware vulnerabilities
	▪ Lax physical security
	▪ Weak policies and procedures

Risk Assessment	Risk assessment is the practice of discerning which threats are relevant to the organization and determining the cost of such threats. 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.
Risk Response	After you have identified the risks and their associated costs, you can determine the best way to respond to the risk. Responses include: ▪ Taking measures to reduce (or mitigate) the likelihood of the threat by deploying security controls and other protections. ▪ Transferring (or assigning) risk by purchasing insurance to protect the asset. When the incident occurs, the cost to the asset is covered by insurance. ▪ 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 the case of the latter, 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 a risk of any level. Risk rejection introduces the possibility of negligence and may lead to liability. ▪ Risk deterrence is letting threat agents know of the consequences they face if they choose to attack the asset. It is not possible to eliminate all risk. Risk management reduces risk to acceptable levels. Risk that remains after reducing or transferring risk is called *residual* risk.