Understanding Risk Management

- Risk refers to a situation involving exposure to danger or the possibility that something unpleasant or unwelcome will happen, with a degree of uncertainty about expected or potential damage that an adverse event may cause to the system or resources.
- Risk Management: a set of policies and procedures to identify, assess, prioritize, minimize, and control risks.
- Risk Assessment: Refers to the identification of risks, the estimation of their impact, and the determination of sources to discern proper mitigation.
- Risk Mitigation: A strategic approach to preparing to handle risks and reduce their impact on the organization.
- Risk Management Plan Evaluation: evaluate and update risk management plans on a regular basis as risks can change with changes in business strategies, policies, and operations.
- Risk Assessment Process:
    - System Characterization: Identify all relevant resources and infrastructure boundaries.
    - Threat Identification: identify possible threats, consider threat sources, potential vulnerabilities, and various security controls.
    - Vulnerability Identification: identify and list all the vulnerabilities in the IT systems that may be maliciously exploited by various threat source.
    - Control Analysis: analyzing various security controls implemented by the organization to eradicate or minimize the probability that a threat will exploit a system vulnerability.
    - Likelihood Analysis: the calculation of the probability that a threat source exploits an existing system vulnerability.

Created by: Abdelrahim Alsadiq

Likelihood	Consequences				
	Insignificant (Minor problem easily handled by normal day-to-day processes)	Minor (Some disruption possible, e.g., damage equal to $500k)	Moderate (Significant time/resources required, e.g., damage equal to $1 million)	Major (Operations severely damaged, e.g., damage equal to $10 million)	Severe (Business survival is at risk, e.g., damage equal to $25 million)
Almost Certain (>90% chance)	High	High	Extreme	Extreme	Extreme
Likely (between 50% and 90% chance)	Moderate	High	High	Extreme	Extreme
Moderate (between 10% and 50% chance)	Low	Moderate	High	Extreme	Extreme
Unlikely (between 3% and 10% chance)	Low	Low	Moderate	High	Extreme
Rare (<3% chance)	Low	Low	Moderate	High	High

- This is a standard risk matrix defined by NIST; organizations need to create their own risk matrix based on their business needs.

- Impact Analysis: involves estimating the adverse impact caused by the exploitation of the vulnerability by the threat source.

Magnitude of Impact	Impact Definition
High	Exploitation of the vulnerability may lead to: ▪ Highly costly loss of tangible assets ▪ Severe damage to the mission or reputation of the organization ▪ Death or severe injury
Medium	Exploitation of the vulnerability may lead to: ▪ Costly loss of tangible assets ▪ Moderate damage to the organization's mission or reputation ▪ Human injury
Low	Exploitation of the vulnerability may lead to: ▪ Loss of a few tangible assets ▪ Light damage to organization's mission or reputation

- Qualitative impact analysis prioritizes the risks involved and identifies the immediate improvement areas.
- Quantitative impact analysis provides the impact's magnitude measurement, which is in turn used for a cost-benefit analysis of the recommended controls.

- Risk Determination: Determine risk based on likelihood, impact, and capability of security controls.
- Control Recommendation: Recommend controls based on the likelihood, impact, and criticality of risk for business operations.
- Risks Assessment Report: Present the results of risk assessment in an official report.

❖ Risk Levels: an assessment of the resulting impact on the network.

Risk Level	Description
Insignificant	Impacts non-critical systems, functions, and processes that can be replaced easily
Minor	Impacts non-critical systems, functions, and processes that are difficult to replace
Moderate	Affects systems, functions, and services containing small amounts of sensitive data
Major	Affects highly sensitive data and resources and impacts business functionality
Severe	Affects mission critical data and resources, and results in severe business and financial losses

❖ A risk matrix is used to scale risk by considering the probability, likelihood, and consequence/impact of the risk.

❖ Risk Mitigation: includes all possible solutions for reducing the probability of the risk and limiting the impact of the risk if it occurs. Has the following strategies:

- Risk Assumption: accepts the potential risk and continues operating the IT system as is.
- Risk Avoidance: preventing risk by curbing the cause of the risk and/or its consequences.
- Risk Limitation: implements controls to diminish the level of controls which in turn condenses the impact of a threat's exercising vulnerability.
- Risk Planning: A risk mitigation plan is to be developed in order to prioritize, implement, and maintain the controls.
- Research and Acknowledgement: vital to analyze the vulnerability of flaw and to evaluate what actions can be taken to correct the vulnerability in order to reduce the loss caused by the risk.
- Risk Transference: transferring the risk and/or getting compensation for losses, such as purchasing insurance and making claims when there are losses.

- Risk Evaluation Plan and Update: requires a tracking and review structure to ensure effective identification and assessment of the risks as well as the use of appropriate controls and responses.
- NIST Risk Management Framework: a structured and continuous process that integrates information security and risk management activities into the system development life cycle (SDLC). Has the following stages:
    - Categorize Select Implement Assess Authorize Monitor: defining the criticality or sensitivity of the information system according to the potential worst-case scenario.
    - Select Security Controls: Categorize the information system, and then select the baseline security controls under a NIST risk management framework.
    - Implement Security Controls: Implement security controls within the enterprise architecture using sound system-engineering practices.
    - Assess Security Controls: Determine security control effectiveness by ensuring correct and effective implementation of the controls as per required operation and compliance with security requirements for the information system.
    - Authorize Information System: Determine risk to organizational operations and assets, individuals, other organizations, and the nation; if acceptable, authorize the operation.
    - Monitor Security State: Continuously track changes to the information system that may affect security controls and reassess control effectiveness.