**RISK ASSESSMENT AND MANAGEMENT**

**Risk management**

-is the process of identifying, assessing and addressing any financial, legal, strategic and security risks to an organization

-practices aim to anticipate these threats and their potential impact and establish plans to address them when they arise.

**Risk Assessment**

* Risk
* Threat
* Vulnerabilities
* Impact

**Threat**

– anything that could cause harm (e.g., hackers, fire, malware). Any potential circumstance or event, whether intentional or accidental, that could negatively impact an organization's information assets by causing unauthorized access, disclosure, modification, destruction, or denial of service.

**Vulnerability**

– a weakness that a threat could exploit (e.g., weak passwords, no backup). A weakness or flaw in a system, software, configuration, or human process that can be exploited by an attacker to compromise the confidentiality, integrity, or availability of data and systems.

**Risk**

– the potential for a threat to exploit a vulnerability and cause an impact. the likelihood and impact of a potential threat exploiting a vulnerability, leading to negative consequences for an organization's data, systems, and reputation.

**Risk is the possibility of loss, damage, or negative impact when a threat exploits a vulnerability.**

**Risk exists only when:**

•There is a Threat (danger)

•There is a Vulnerability (weakness)

•The Threat can exploit the Vulnerability, leading to an Impact

**Impact**

* the consequence or damage if the threat succeeds (e.g., data loss, service disruption). refers to the harm resulting from the unauthorized disclosure, modification, destruction, or loss of information, or the unavailability of an information system.
* is the effect or consequence on the organization if a threat successfully exploits a vulnerability. In simple terms: “What will happen if the risk occurs?”

•Threat = Danger

•Vulnerability = Weakness

•Risk = Threat + Vulnerability

•Impact = What happens if risk occurs

The Risk Formula:

Risk = Threat × Vulnerability× Impact

Types of Risk in Information Security & Business

Based on Level of Severity

•High Risk – Very likely to happen and will cause major damage. Example: Outdated POS system gets hacked → huge customer data breach.

•Medium Risk – Possible to happen and will cause moderate damage. Example: Weak passwords used by some staff → limited system misuse.

•Low Risk – Rare to happen or will cause minimal damage. Example: Occasional slow Wi-Fi in the store → slight inconvenience.

Based on Business Areas

•Reputational Risk – Risks that affect profit, reputation, or customer trust.

•Operational Risk – Risks affecting daily store operations.

•Financial Risk – Risks involving money or penalties. •Cybersecurity Risk – Risks targeting digital systems and data

•Compliance / Legal Risk – Risks from not following laws/regulations

•Physical Risk – Risks from physical damage or theft.

Types of risk:  
Financial risk

* includes issues that are related to changes in market conditions, interest rates, exchange rates and other factors.

Strategic risk

* is associated with poor business decisions, ineffective strategies or inadequate responses to technological changes or shifts in customer behavior.
* Project risks
* related to market competition, including mergers and acquisitions, entry into new markets or the launch of new products, are considered strategic risks.

Operational risk

* as a category includes both internal and external threats. Internal problems such as human error, technology and system failures, and operational inefficiencies can hurt an organization’s ability to meet its obligations and goals.

Cybersecurity risks

* include data breaches, cyberattacks, phishing attempts and issues of unauthorized access to company systems or information.

Compliance risk

* involves issues with following laws, regulations, and standards. Failure to keep up with evolving regulatory rules or monitor internal processes can lead to legal and financial problems.

Reputational risk

* includes anything that damages an organization's public face, such as negative publicity, customer dissatisfaction or ethical issues.

Risk Treatment

Risk avoidance

* means not participating in activities that might negatively affect the organization.

Risk reduction

* accepts risk but aims to minimize it and its impacts. Risk reduction accepts the risk but focuses on keeping any loss from spreading.

Risk sharing

* Involves transferring some or all of the risk to another party. A corporation is a good example of risk sharing, several investors pool their capital and each bears only a portion of the risk that the enterprise will fail.

Risk transfer

* involves contracting a third party to absorb the risk.

Risk acceptance and risk retention

* involve accepting the potential consequences of risk and preparing to manage them if they occur.

Steps of the risk management process

Risk management processes

* involve the people, technology and behaviors that help an organization to address risks and reach its objectives.

4 key steps in any risk management plan include:

* Risk identification
* Risk assessment
* Risk mitigation
* Risk monitoring

Risk identification

* is the process of recognizing potential threats to an organization, its operations and its workforce.

Risk assessment

* focuses on analyzing and evaluating potential risk factors.

Risk analysis

* involves establishing the probability that a risk event might occur and the potential outcome of each event.

Risk evaluation

* compares the magnitude of each risk and ranks them according to prominence and consequence.

Risk mitigation

* involves developing and implementing strategies to address and control an organization’s risk. It entails risk control actions that are put into place to deal with risk factors and the effects of those actions on the advancement of projects or goals.

Risk management

* is a nonstop process that adapts and changes over time. Repeating and monitoring the process can help organizations keep up to date on new risks.

•Risk Management = The whole process of dealing with risks (planning and execution).

•Risk Monitoring = The watchdog activity that ensures risks and controls are continuously tracked and adjusted.

Types of risk management

* Cyber risk management
* AI risk management
* Model risk management
* Supply chain risk management
* Third-party risk management
* Artificial intelligence in risk management

Cyber risk management

* also called cybersecurity risk management, involves protecting an organization's digital assets and information technology.

AI risk management

* addresses the potential risks that are associated with artificial intelligence technologies.

Model risk management (MRM)

* involves validating models and tools before and after they are implemented and adjusting throughout their lifecycle to protect their integrity.

Supply chain risk management (SCRM)

* aims to identify vulnerabilities in the supply chain and minimize their impact on a company's operations, reputation and financial performance.

Third-party risk management (TPRM)

* addresses risks associated with outsourcing tasks to outside vendors or service providers. These third-party partnerships might be involved in functions, such as IT services, supply chain management or customer support.

Artificial intelligence (AI) and machine learning (ML) technologies support risk management

* programs by helping organizations proactively identify and mitigate potential threats. Risk management specialists and other risk professionals can utilize AI tools and systems to effectively detect problems and automate solutions.

Natural language processing (NLP)

* NLP tools can be used to analyze unstructured data sources, such as news articles, social media or customer interactions, and identify any risks that might impact an organization

**Risk management standards and Framework**

**ISO 31000**

* Developed by the **International Organization for Standardization (ISO).** It provides principles, a framework, and a process for managing risks, applicable to any organization regardless of size, activity, or industry.

**COSO Enterprise Risk Management (ERM) Framework:**

* Developed by **the Committee of Sponsoring Organizations of the Treadway Commission (COSO),** this risk management framework provides guidance on integrating risk management into an organization's strategy and performance.

NIST Cybersecurity Framework

* Developed by the US Department of Commerce’s **National Institute of Standards and Technology (NIST),** it provides guidance on managing cybersecurity risks. It is flexible, and can be applied to organizations of any size, industry, or sector.

GRC Capability Model

* Developed by the Open Compliance and Ethics Group (OCEG), it provides guidelines for integrated governance and compliance. It’s sometimes known as the OCEG Red Book.