Information Risk Management and Security: A Stategic Overview

Risk management is the process of identifying, assessing, and controlling threats to an organization's assets, operations, and goals. In a business environment, managers are expected to align operational decisions with the broader objective of minimizing risk exposure. They use specific tools and models to evaluate the quantify the risk associated with external threats, system vulnerabilities, and business processes.

Quantitative risk assessment is a mathematical approach to determining risk. This technique calculates potential loss associated with a given risk by combining the likelihood of an event with the expected impact. Tools such as Annualized Loss Expectancy (ALE), Single Loss Expectancy (SLE), and Annual Rate of Occurrence (ARO) are frequently used. These allow management to evaluate alternate course of action and assign financial values to various risk scenarios.

Qualitive risk assessment, in contrast, does not use numerical formulas. It is based on expert judgment, experience, and likelihood-impact metrics. It involves categorizing risks according to severity and probability and especially useful when precise data is available. Qualitative risk methods often involve brainstorming, interviews, and SWOT analysis to identify and prioritize risk.

Information security refers to the protection of an organization's information assets from unauthorized access, disruption, or destruction. Its core principles—confidentiality, integrity, and availability—are often referred as the CIA triad. This concept ensures that

only authorized individuals can access sensitive data (confidentiality), data remains accurate and unaltered (Integrity), and systems remain accessible to users when needed (availability).

While information security deals with the protection of the information, risk management encompasses a broader scope. It includes financial, operational, reputational, and regulatory risks in addition to information systems. Information security is thus one component of a comprehensive risk management strategy.

Security policies form the foundation of an organization's security strategy. These policies provide a high-level overview of how security is managed and enforced. They serve as formal statements from management that set expectations for employee behavior and IT operations. Examples include acceptable use policies, data classification policies, and incident response plans.

Some principles underlying effective security policies include proportionality (Investing in protection proportional to asset values), access control (limiting user access based on job), and least privileged (granting users only permissions they need to perform their jobs). In addition, automation can help reduce human error, and input validation can mitigate software vulnerabilities.

Employes's must be trained to recognize threats such as phishing, social engineering, and malware. Antivirus software, intrusion detection systems (IDZ), firewalls, and security information and event management (SIEM) tools should be in place to provide boundary protection. Security policies are crucial in defining how risk is managed in an organization.

They help identify threats, establish control measures, and assign responsibility. Without policies, risk management lack's structure and guidance.

Both IT and non-IT leaders have roles to play in risk management. IT leaders are responsible for identifying technological threats and designing technical safeguards such as encryption, multifactor authentication (MFA), and intrusion prevention systems. They also draft security policies and oversee compliance with industry standards.

Non-IT leaders, on the other hand, must ensure that these policies are understood and followed within their departments, they act as intermediaries between technical teams and executive management. Communication between IT and business units is essential to align cybersecurity efforts with organizational goals.

ISCA Journal emphasizes that non-IT managers can champion IT risk management and foster cross-functional cooperation. Similarly, Info security Europe reports that executive leadership plays a key role in allocating resources for cybersecurity initiatives and making strategic decisions. Tailored risk management plan should begin by identifying the organization's risk tolerance. This includes defining what levels of risk are acceptable, determining risk appetite, and clarifying strategic priorities. Next, the plan should identify potential internal and external threats such as natural disasters, insider threats, and cyberattacks.

Thes risks must then be assessed using qualitative and quantitative methods. The result is a prioritized list of risks that can be addressed using technical controls, administrative

policies, training or insurance. Each recommended mitigation strategy should be accompanied by a cost-benefit (CBA) to justify the investment.

The plan must assign accountability and define escalation procedures. Risk management is a continuous process—it should evolve to reflect changes in technology, business strategy, and the threat landscape.

In conclusion, effective information risk management depends on the strong policies, clear communication, cross-functional responsibility, and ongoing adaption. By understanding the relationship between information security and risk management, leaders can protect data and business value.

Practical Risk Management Measures:

- Purchasing Insurance – Reduce the impact of threats by transferring financial risk.
- Access controls – Apply the principle of least privilege and need-to-know
- Automation – Automate routine processes to reduce human error.
- Input validation – ensure all user and system inputs are validated for correctness.
- Training – Provide employee training to recognize and respond to threats.
- Antivirus software – Detect and remove malicious software and prevent infections.
- Boundary protection – Implement firewalls, IDS/IPS, and SEIM systems for defense.

ALLISON, J. Cybersecurity Risk Management Scenarios for Teaching Information Security Management. **Journal of Applied Security Research**, *[s. l.]*, v. 20, n. 2, p. 167–188, 2025. DOI 10.1080/19361610.2024.2358272. Disponível em:

.

Acesso em: 20 jul. 2025.

Gibson, D., & Igonor, A. (2020). *Managing risk in information systems* (3rd ed.). Jones & Bartlett Learning. Available from Strayer University Bookshelf.

NIKLAS HUMBLE. Risk management strategy for generative AI in computing education: how to handle the strengths, weaknesses, opportunities, and threats? **International Journal of Educational Technology in Higher Education**, *[s. l.]*, v. 21, n. 1, p. 1–35, 2024. DOI 10.1186/s41239-024-00494-x. Disponível em: https://research-ebsco-com.libdatab.strayer.edu/linkprocessor/plink?id=74f33ed3-2a0a-3081-938a-d1e63576eef7. Acesso em: 20 jul. 2025.