Funded by the European Union

secureu
DIGITAL EDUCATION TOOLS FOR SECURITY RISK MANAGEMENT

SELECTION OF CYBERSECURITY TECHNOLOGIES BASED ON RISK MANAGEMENT PROCESSES

Jyri Rajamäki / Laurea University of Applied Sciences, Finland / 2023

ABSTRACT

By following the principles of ISO 31000:2018, organizations can make informed decisions about the selection, implementation, and ongoing management of cybersecurity technologies to effectively mitigate risks and protect their information assets. Drawing on the results of the DIMECC Cyber Trust programme, this article provides a structured approach to choosing the necessary security technologies based on risk management processes, which is crucial in the context of ever-evolving cybersecurity threats.

Link to ISO 31000

Parts from ISO 31000:2018 Risk management process referenced in this article Risk Assessment, Risk Treatment, Monitoring and Review, Recording and reporting, Communication and Consultation

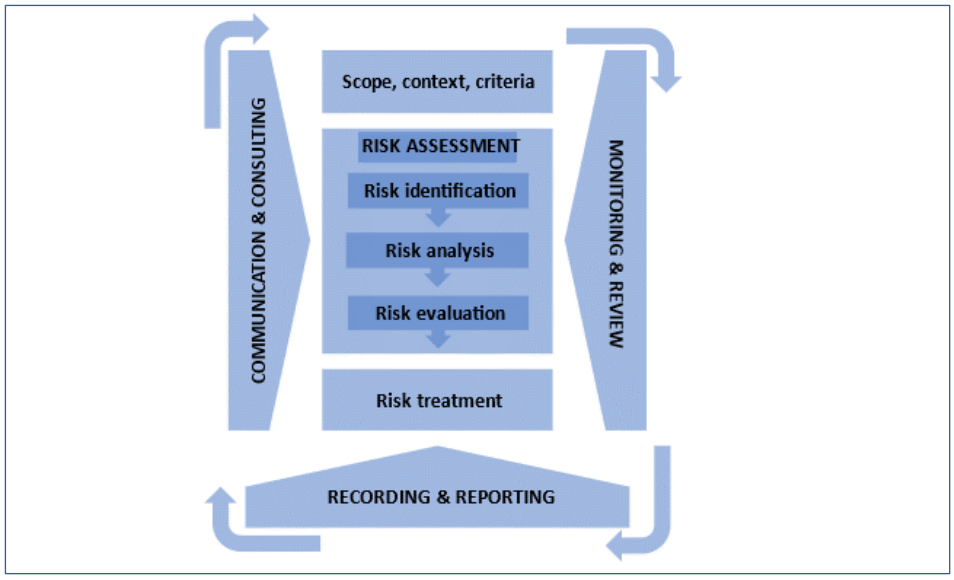

Figure 1. Risk management process (adapted from ISO 31000:2018)

1. Introduction

Risk management is an essential part of setting strategy, achieving objectives, and making decisions at different levels of the organization. ISO 31000:2018 provides guidelines and principles for effective risk management in any organization. Risk management has a vitally important role in any

management system. For example, in practice, cybersecurity management is a risk management procedure as the Figure below illustrates.

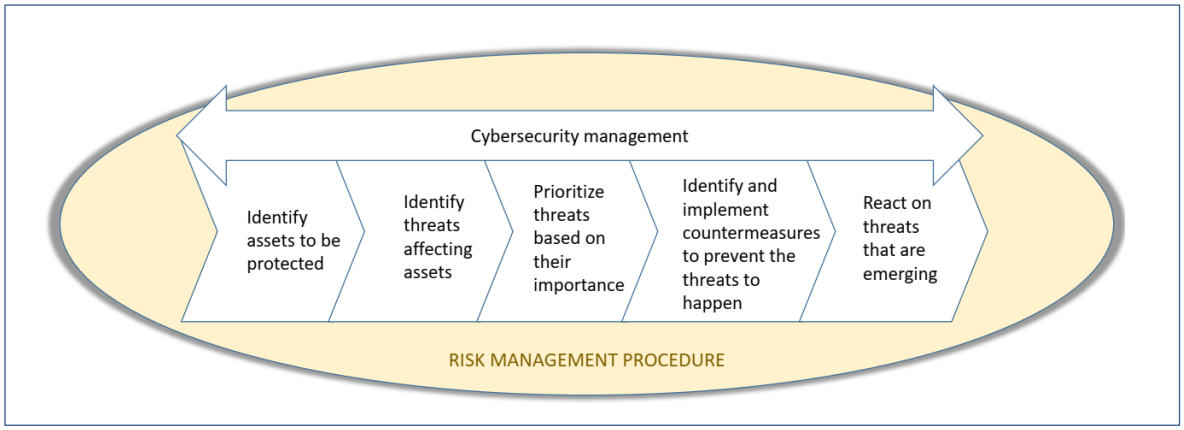

Figure 2. Cybersecurity as a risk management procedure (adapted from Rajamäki & Nevmerzhitskaya, 2018)

Security technologies encompass technical means for achieving cybersecurity, including secure system architectures, protocols, and tools. They enable the protection of infrastructures, platforms, devices, services, and data. Key aspects include user identification, authorization, and access rights. Common security technology standards include ISO/IEC 27033 for network security and ISO/IEC 27034 for application security. While ISO 31000 doesn't specifically address cybersecurity technologies, its principles and framework can be applied to the selection and implementation of cybersecurity technologies within an organization.

2. Case

The DIMECC Cyber Trust Programme created a foundation for Finnish research and industry to address needs emerging within cybersecurity. The main research objective of the DIMECC Cyber Trust programme was to improve privacy, trust, and decision-making within digital infrastructure. The consortium consisted of 19 companies and 8 research institutes and universities. The programme published over 130 research articles on cyber security and how to protect privacy.

Cybersecurity serves as a key enabler of trust development in the digital world, to ensure resilience in all operational systems and infrastructures. DIMECC outlines four key themes within cybersecurity, namely security management, situational awareness, security technologies, and resilience of operational systems.

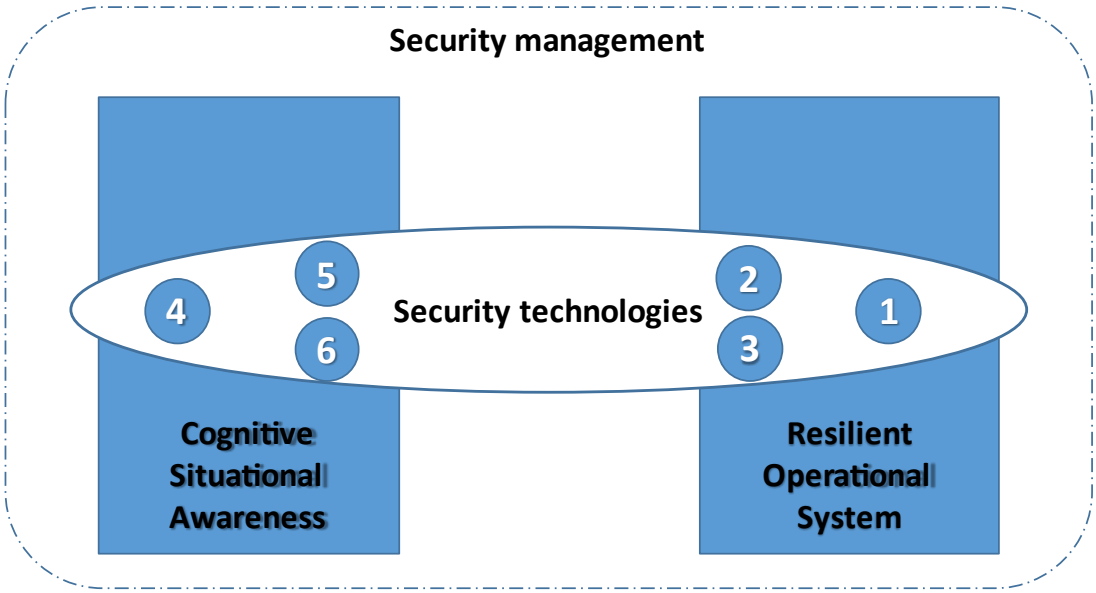

Figure 3. Categories of cybersecurity technologies (adapted from Rajamäki, 2022)

Security technologies can be divided into six different categories according to their goal:

1. Technologies for Improving the security of the operational system, such as system architectures, protocols, implementations, development tools, and development platforms.
2. Protection technologies, such as user identification and authorization, firewalls, antivirus programmes, intrusion protection systems (IPS), and security information and event management (SIEM) systems.
3. Technologies for producing security data, such as sensors (firewall logs, system event logs, antivirus, and packet capture) network traffic analyzers, intrusion detection systems (IDS), and open-source intelligence (OSINT) technologies.
4. Technologies for analyzing security data. These technologies can be divided into three levels:
    1. Level1 - History: Forensic
    2. Level2 - Comprehension of the current situation (Data fusion, SIEMs)
    3. Level3 - Projection of future status
5. Technologies for visualising the situational picture, including technologies for human machine interface.
6. Technologies for cyber threat intelligence sharing between organizations, such as early warning systems, Malware Information Sharing Platform (MISP), Cortex, and TheHieve.

It must be noted, though, that several technologies belong to more than one category.

3. Best practices

By combining the information security technologies mentioned with the ISO 31000 processes, a solid cyber security framework can be created. Here are the main aspects of this integrated approach:

1. Risk Identification, Assessment, and Treatment:

- Risk Identification (ISO 31000 - Clause 5):
  - Utilize technologies for producing security data (sensors, network traffic analyzers, IDS, OSINT) to identify potential threats and vulnerabilities.
  - Leverage open-source intelligence technologies for understanding the cybersecurity landscape.
- Risk Assessment (ISO 31000 - Clause 6):
  - Combine technologies for analyzing security data (Forensic, Data Fusion, SIEMs) to assess the likelihood and impact of identified risks.
  - Utilize technologies for visualizing the situational picture to comprehend the current cybersecurity situation.
- Risk Treatment (ISO 31000 - Clause 7):
  - Select and implement protection technologies (firewalls, antivirus, IPS, SIEM) based on the cybersecurity risks assessed.
  - Use technologies for cyber threat intelligence sharing (early warning systems, MISP, Cortex) to stay informed about evolving threats.

2. Monitoring and Review:

- Monitoring and Review (ISO 31000 - Clause 8):
  - Employ technologies for continuous monitoring of the security infrastructure (sensors, IDS).
  - Analyze security logs using technologies for analyzing security data (SIEMs) to identify anomalies.
  - Regularly review and update cybersecurity measures based on the evolving threat landscape.

3. Communication and Consultation:

- Communication and Consultation (ISO 31000 – Clauses 2 and 3):
  - Establish a human-machine interface using technologies for visualizing the situational picture to facilitate communication.
  - Use technologies for cyber threat intelligence sharing to exchange threats and mitigation strategies with other organizations.

4. Integration with Overall Management:

- Integration with Overall Management (ISO 31000 - Clause 4):
  - Integrate cybersecurity risk management into the overall governance using technologies for improving the security of the operational system.
  - Align cybersecurity considerations with business objectives using protection technologies and risk treatment options.

This integrated approach ensures a comprehensive cybersecurity strategy that combines the strengths of various security technologies and aligns with the ISO 31000 processes for risk management. Regular updates and communication channels help in adapting to the dynamic nature of cybersecurity threats.

References

DIMECC Cyber Trust Program. In: dimecc.com [online] [cit. 12/11/2023] Available at: https://cybertrust.dimecc.com/

ISO 31000 Risk management. In: ManagementMania.com [online]. Wilmington (DE) 2011-2023, 11/11/2016 [cit. 12/11/2023]. Available at: https://managementmania.com/en/iso-31000-risk-management

Jyri Rajamäki (2022). Turvallisuusteknologiat kyberympäristön luottamuksen työkaluina. In: *Jatkuvuutta turvaamassa – LaureanYAMK opiskelijoiden näkökulmia*, ed. Harri Ruoslahti, Laurea-ammattikorkeakoulu, pp. 55-64.

Jyri Rajamäki and Julia Nevmerzhitskaya (2018). Cybersecurity in an organization. In: *Organization and individual security*, ed. Ivita Kīsnica, Nordplus, Riga, pp. 539-554.