Risk-Based Prioritization of Cybersecurity Measures for SMEs

Stavros Kousidis

Bachelor thesis · Published: 2026-10-15

Research question

How can a small or medium-sized enterprise prioritize cybersecurity measures under limited resources while accounting for its risk exposure and applicable regulatory requirements?

Description

Small and medium-sized enterprises face cybersecurity risks and a growing body of regulatory and technical guidance. Existing publications already describe many recommended measures. The challenge addressed here is deciding which measures are appropriate for a particular organization, in which order, and with what justification.

You will investigate selected guidance and develop a method for prioritizing a manageable set of technical and organizational security controls. The method should explicitly consider an organization's assets, exposure, dependencies between measures, implementation effort, and available resources. Relevant European frameworks, including NIS2, the Cyber Resilience Act and the EU Cybersecurity Act, must be distinguished by scope and applicability; they are not interchangeable compliance checklists.

Scope and evaluation

Focus on one clearly specified SME profile or business category. Define a small number of realistic scenarios and compare your prioritization with a documented baseline, such as a fixed checklist or established control ordering. Examine sensitivity to changes in assumptions, budget and risk estimates. The goal is to evaluate the method, not to claim that its output certifies legal compliance.

Expected outcome

A transparent prioritization method, worked scenarios, and an evidence-based evaluation of its usefulness and limitations. An implementation roadmap may accompany the results.

Starting points

- ENISA: Cybersecurity Guide for SMEs.
- ENISA: NIS2 Technical Implementation Guidance.
- European Commission: Cyber Resilience Act.
- ENISA, *Cybersecurity for SMEs: Challenges and Recommendations* (2021).

Contact: stavros.kousidis@th-koeln.de
Code publication: open source by default; exceptions require prior agreement (policy).