Adapting Cybersecurity Frameworks for NIS2 Compliance

University of Turku
Department of Computing
Master of Science (Tech) Thesis
Cyber Security Engineering
April 2025
Andrew Bowo

Supervisors:
Antti Hakkala
Petri Sainio

UNIVERSITY OF TURKU
Department of Computing

Andrew Bowo: Adapting Cybersecurity Frameworks for NIS2 Compliance

Master of Science (Tech) Thesis, 67 p., 7 app. p.
Cyber Security Engineering
April 2025

This thesis examines the role of cybersecurity maturity evaluation in addressing the current level of cybersecurity and identifying necessary measures to reach compliance with the Network and Information Security Directive 2 (NIS2), which requires entities critical to society to adopt and maintain specific measures to ensure resilience against cyber threats. By analyzing the current cybersecurity landscape, identifying the requirements of the NIS2 Directive, and conducting an assessment using Kybermittari, this thesis highlights the strengths, weaknesses and practical implications of using maturity models for NIS2 compliance, while also demonstrating how cybersecurity models can be used to evaluate and improve information security and compliance. The findings show that assessments are an effective way to evaluate an organization's cybersecurity capabilities and support the efforts in reaching compliance with the NIS2 Directive. It also emphasizes the significance of in-depth understanding of the organizations operations and commitment of personnel, as well as towards actionable improvement plans to enhance cyber resilience and prepare for the next evaluation.

Keywords: information security, NIS2 Directive, cybersecurity maturity models, Kybermittari, risk management, cyber incident

Contents

List of Figures

List of Tables

List of acronyms

C2M2 Cybersecurity Capability Maturity Model

CEN/TS European Committee for Standardization/Technical Specification

CSF Cybersecurity Framework

CSIRT Computer Security Incident Response Team

DDoS Distributed Denial of Service

DNS Domain Name System

ENISA European Union Agency for Cybersecurity

ETSI European Telecommunications Standards Institute

EU-CyCLONe European Cyber Crisis Liaison Organization Network

GxP Good Practices for regulated industries

ICT Information and Communication Technology

IEC International Electrotechnical Commission

ISMS Information Security Management System

ISO International Organization for Standardization

MaaS Malware as a Service

MFA Multi-Factor Authentication

NCSC National Cyber Security Centre

NCSI National Cyber Security Index

NIS Network and Information Systems

NIST National Institute of Standards and Technology

OT Operational Technology

SME Small and Medium-sized Enterprise

1 Introduction

In the modern digital age, the sophistication and frequency of cyberattacks pose significant challenges for organizations around the world. Reports indicate a notable increase in both the frequency and financial impact of cyber incidents on organizations. For instance, according to IBM's Cost of a Data Breach Report 2024, the global average cost of a data breach in 2024 stands at USD 4.88M with a 10% increase compared to the previous year [1]. This, in combination with 11,079 incidents observed in the EU; a 329% increase between 2023 and 2024 [2], [3] highlights the need for more robust cybersecurity policies in the EU.

Recognizing the need for robust and consistent cybersecurity measures across member states, EU has taken steps to address the evolving landscape of cybercrime with the revised Network and Information Security Directive (NIS2), extending its scope to more sectors. By emphasizing enhanced measures for risk management, reporting obligations, and resilience, NIS2 holds essential and important industries, as well as their top management, accountable for their own cybersecurity. While the NIS2 Directive mandates organizations to adopt certain specific measures to ensure resilience against cyber threats, it doesn't directly provide the means or detailed methodologies to evaluate and achieve the desired state or controls to comply with the requirements. [4]

Organizations may face issues with implementing the requirements outlined in the directive, due to a lack of understanding regarding the extent and efficiency of

their existing cybersecurity measures. By individually interpreting and implementing the requirements based on the organization's unique contexts, inconsistencies may appear regarding how organizations approach compliance. And as disproportionate and insufficient implementations, unclear definitions and lack of cooperation between member states was recognized as crucial shortcomings of the initial Network and Infrastructure Directive [5], the need for standardized metrics to assess organizations cyber resilience becomes evident.

Cybersecurity maturity models provide a structured approach for organizations to evaluate their cyber resilience, identify weaknesses and maintain an operational structure that considers all hazards [6]. A suitable maturity model can be used as a tool to address the gaps and necessary measures to reach compliance with the NIS2 requirements effectively. This thesis aims to bridge the gap between the NIS2 Directive's requirements and the existing maturity assessment frameworks by studying their applicability, effectiveness and extent in relation to the listed topics in the NIS2 Directive.

1.1 Objectives and Scope

This thesis aims to explore the requirements set by the EU and Finland in response to the increasing cybersecurity challenges, with a particular focus on the NIS2 Directive. The primary objective is to utilize cybersecurity maturity models to assess organizations' current levels of resilience, sophistication, and identify critical gaps. By evaluating these challenges in the context of the NIS2 Directive, the thesis seeks to provide insights into how organizations can improve their cybersecurity posture and ensure compliance.

The scope of this thesis includes providing a comprehensive understanding of the NIS2 Directive and its implications for organizational cybersecurity. The result will provide a theoretical basis and practical approaches for improving cybersecurity

resilience, whether the goal is to achieve compliance with the NIS2 Directive, prepare for future regulatory requirements, or strengthen overall cybersecurity posture.

A key part of this research is the practical application of cybersecurity maturity assessments, illustrated through a case study for a manufacturing company as part of their efforts to ensure compliance with the NIS2 Directive. Additionally, the thesis evaluates various maturity models, examining how they align with the requirements of the NIS2 Directive and assessing their effectiveness in addressing key cybersecurity challenges. The aim is to demonstrate how a maturity assessment can be conducted and to highlight its benefits in improving organizational security.

Through this analysis, the thesis will emphasize the value of maturity assessments as a tool for strengthening cybersecurity strategies, ensuring compliance, and preparing organizations for future regulatory and security challenges. With these remarks, this thesis will focus on answering the following research questions.

1. How can cybersecurity maturity models be used to evaluate and improve organizations' information security and compliance with the NIS2 directive?

2. What are the strengths, weaknesses, and applicability of cybersecurity maturity models in the context of NIS2 requirements?

1.2 Structure of the thesis

The later chapters of this thesis are organized as follows: Chapter 2 provides insights on the subject matter, focusing on the current cybersecurity landscape, trends, and targeted sectors. Chapter 3 introduces the Network and Information Security Directives, their objectives, and the adaptation of NIS2 to Finnish legislation, while also detailing the implications for organizational cybersecurity. Chapter 4 defines maturity models and presents key frameworks and their relevance in the context of NIS2. Chapter 5 discusses the design of the case study and how the evaluation is

conducted. Chapter 6 presents the insights gathered from the maturity assessment process, discusses the findings of the maturity assessment and provides a reflection on the results of the conducted work. Chapter 7 concludes the thesis with a summary, implications, key takeaways, and final reflections.

2 Cybersecurity Context

This chapter aims to provide a comprehensive review of the current situation regarding cybersecurity as of 2024. By examining the evolving cybersecurity landscape from local to global perspectives, a clear picture can be presented, supported by relevant statistics and observations on current key trends. Particular focus is given to the most affected industries and targeted sectors, with manufacturing being the most critical.

2.1 Global and EU Threat landscape

As discussed in Chapter 1, the amount of cyber-related incidents has steadily increased in recent years, with a notable increase in the European Union. While the World Economic Forum's global risks report indicates that cyberattacks are perceived as the fifth most likely risk to present material crisis [7], the world's dependency on digital infrastructure cannot be underestimated. This was further demonstrated by the CrowdStrike incident, which affected 8.5 million Windows devices and caused widespread disruption for organizations [8].

While malicious and unintentional disruptions in services and operations have become more frequent, progress has been made in terms of legal, technical, organizational, capacity-development and cooperative measures regarding cybersecurity. Between 2020 and 2024, the Global Cybersecurity Index measurement in these domains across 194 countries has seen a 27% increase in cybersecurity commitment,

indicating that countries have acknowledged the importance of cybersecurity-related measures. [9]

Geopolitical tensions present in the EU and mainly caused by Russia's war of aggression against Ukraine, coupled with increased hacktivism and the increasing sophistication and scale of attacks, have made cybersecurity crucial for protecting government institutions, including the important and essential entities associated with them. The European Network and Information Security Agency's (ENISA) Threat Landscape 2024 report highlights a significant increase in both variety and quantity of cyberattacks in the EU, with 11,079 observed incidents between July 2023 and June 2024 [3]. Compared to last year's 2,580 observed incidents [2], this represents a significant increase in the number of reported incidents. As seen in Figure 2.1, threats to availability (DDoS) at 41.1% and ransomware attacks at 25.7% are the most common of the observed incidents.

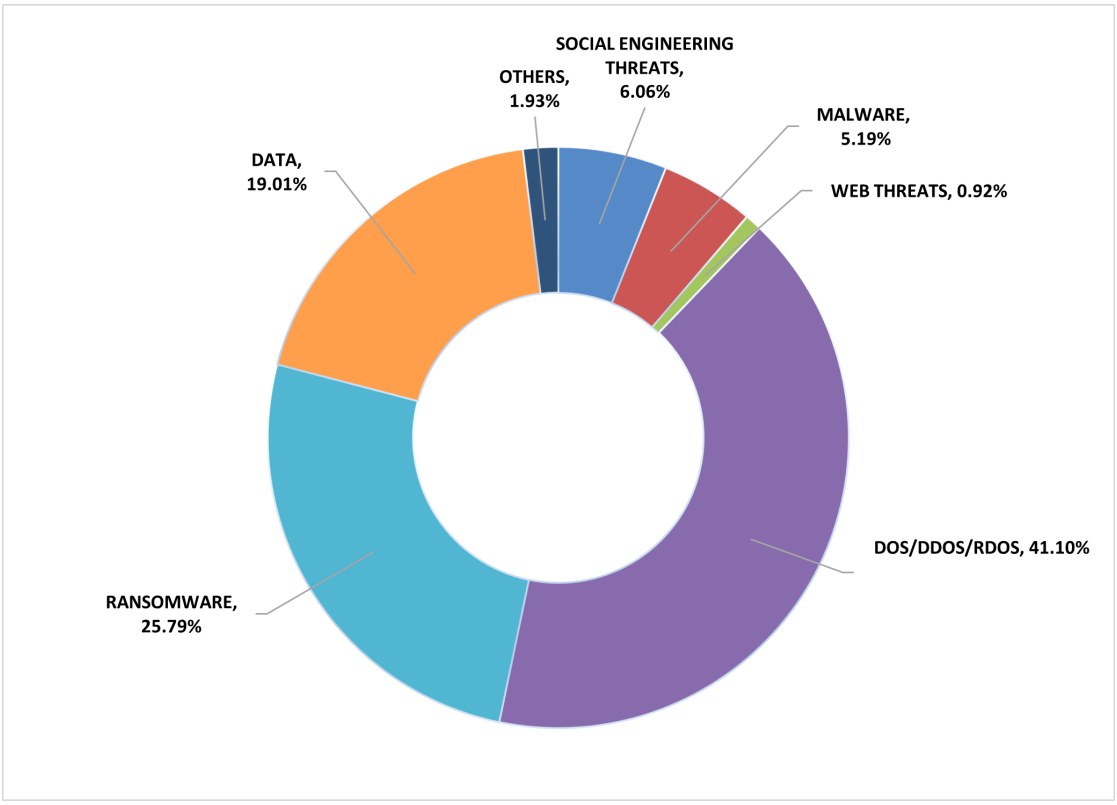

Figure 2.1: Distribution of Cyber Incidents in the EU (July 2023—June 2024). Adapted from ENISA [3].

2.1.1 Threat landscape in Finland

Finland has been recognized as the 13th most resilient country globally in terms of its capacity to prevent cyber threats and manage cyber incidents, based on data collected from 2016 to 2023 by NCSI [10]. This recognition reflects Finland's strong cybersecurity infrastructure and its ongoing efforts to enhance preparedness and response capabilities in the face of evolving cyber risks. Despite Finland's strong posture, an increasing amount of cyberattacks has been observed, with 44% increase in reported incidents from 2022 to 2023. These were driven by a surge in phishing, data breach attempts, and fraud campaigns.

A particularly notable attack was allegedly orchestrated by the group NoName057(16), targeting the Finnish Parliaments website on April 4, coinciding with Finland's accession to NATO [11], [12]. This underscores the politically motivated nature of modern cyberattacks, where symbolic institutions are targeted to further political and ideological agendas.

Additionally, the increasing sophistication and more targeted approach in attacks affect a wider range of entities. It has been observed that attackers utilize a wider range of tools and utilize automatization in carrying out the attacks and this was particularly evident in the rise of denial-of-service attacks during the late fall of 2023. In total, 1,014 breaches and 18,625 information security anomalies were observed by Traficom in 2013 [12].

2.2 Cyber Key Trends

The key trends observed in the cyber threat landscape highlight the increased utilization of technological and strategic advancements in malicious activities. Stealth techniques like Living Off Trusted Sites (LOTS) are increasingly being exploited, where trusted sites are utilized to carry out attacks and malicious content [13]. In

addition, geopolitics remain a strong driver for malicious operations, with governmental backing. [9]

From a technological standpoint, the usage of artificial intelligence has also been recognized as a growing threat vector. Generative tools such as FraudGPT and WormGPT have emerged to help cybercriminals run automated phishing campaigns and generate malware able to bypass traditional virus detection systems [3], [14].

From a societal perspective, information manipulation can also be detected as an evolving threat. The possibilities of artificial intelligence enabled information manipulation increases the potential of spreading misleading or false information to large masses. Beyond political agendas, such manipulation can result in harmful, inaccurate reports that may incite actions detrimental to governments or public order.

In addition, the rise of Malware-as-a-Service (MaaS) offerings and increasing usage of DDoS-for-Hire services illustrate the growing involvement of unskilled users in cyberattacks. As these services enable those with limited technical expertise to utilize sophisticated tools and resources, the barrier to entry in malicious activities keeps lowering. [3]

2.3 Targeted Sectors

According to the European Repository of Cyber Incidents, between January 1, 2023 and December 2, 2024, the critical infrastructure stands as the most targeted sector globally, accounting for 58.1% of all observed incidents. The health sector followed as the most affected sector, representing 14.9% of attacks on the critical infrastructure sector. Corporate entities were another significant target, with 9% of incidents directed at this sector. [15]

Aligning with ENISA's assessment of the EU's cyber threat landscape, the tension is evident in public administration, which has become the most targeted sec-

tor, accounting for 19% of recorded incidents, while attacks on the healthcare and manufacturing sectors have also increased both individually and through the cascading effects of a single event affecting several sectors at once. From the standpoint of affected sectors, the observed events recognized by the ENISA highlight interconnectivity, particularly concerning the digital infrastructure, manufacturing, and business services sectors as they have an impact on other sector groups. [3]

A closer inspection of the manufacturing sector reveals its vulnerability towards significant threats, with ransomware and DDoS attacks being particularly prominent. Although a decline in supply chain attacks has been observed by ENISA [3], manufacturing remains a critical target due to its heavy reliance on automation, its integral role in supporting critical infrastructure, and the integration of IT and operational technology (OT) environments. These factors make it highly attractive to cybercriminals, especially as advanced toolkits like Pipedream have gained recognition and are being employed to target OT systems with cross-industry disruptive and destructive malware [16], [17].

In addition, the scale of operation and limited tolerance for downtime in the manufacturing industry have resulted in a continued reliance on human-operated systems and legacy technologies, increasing its susceptibility to cyberattacks. According to the IBM X-Force Threat Intelligence Index 2024 report, the manufacturing industry in Europe has become the most attacked industry, accounting for 28% of incidents [18].

Despite advancements in both offensive and defensive cybersecurity strategies and technologies, human error remains a critical threat vector. Credential mishandling, social engineering, and weak password practices were observed as the most common entry point into victim environments, accounting for 30% of incidents recognized by IBM [18].

The impact of human error is also highlighted by the amount of observed initial

access vectors that could have been mitigated with best practices and security fundamentals. Accounting for 84% of preventable incidents in critical infrastructure, security misconfigurations, abundance of patch management and lack of credential hardenings were observed as the main causes of invasion, highlighting the importance of comprehensive cybersecurity training. [18]

In conclusion, while progress has been made globally in regards acknowledgment, dedicated controls, and actions regarding cybersecurity, the threats and increase in attacks indicate that more robust measures are needed. With a particular focus on the manufacturing sector, the NIS2 Directive identifies manufacturing companies essential for societal and economic stability, highlighting the increasing pressure on these industries to strengthen their cybersecurity defenses.

3 NIS and NIS2 Directives

3.1 NIS Directive

On the 6th of July in 2016, the Network and Information Systems Directive was adopted to establish a unified cybersecurity policy within the EU. Recognizing the economic and societal impact of cyberattacks globally and within Member States, the Directive aimed to provide a foundation on how to achieve a common level of cybersecurity across the EU, while taking into account the cross-border nature of cybersecurity and cooperation between Member States. [5]

3.1.1 Objectives and Reception

Due to the increased magnitude, frequency and impact of security incidents targeted at network and information systems and their essential role in enabling the seamless movement of goods, services, and people across borders within the EU, the existing resources and strategies for protection were found to be inadequate. In addition, the fragmented approaches across the Union had resulted in unequal and uncoordinated levels of protection. The individual approaches of operators of essential services and digital service providers were recognized as problematic, particularly in terms of achieving effective mechanisms for cooperation, communication, and incident tracking. Most notably, the lack of a general cybersecurity policy within the EU made it more difficult to respond effectively to the growing cyber threats, making it chal-

lenging to communicate and alert other member states about emerging attacks and receive timely assistance. [19]

The directive outlined a requirement to identify and document the entities providing essential services, i.e., critical entities that are crucial to the state's infrastructure and economy and engage in bilateral or multilateral cooperation with other Member States. According to the criteria established in Article 5 of the NIS Directive [19, Art. 5] , the operators of essential services are defined as the entities which provide services essential for maintenance of critical societal and/or economic activities, are dependent on network and information systems and would have a significant disruptive effect upon an incident.

The identified operators of essential services were required to be reviewed and updated at least every two years by the Member states. This, in addition to the requirement of adopting cybersecurity strategies, designating crisis management authorities and single points of contact formed the core of the Directive.

The initial NIS Directive was considered successful at increasing awareness of cybersecurity, establishing a foundation for national cybersecurity strategies and encouraging Member States to cooperate in areas such as information sharing and establishing trusted communication channels. Eventually, its practical implementation turned out to be more problematic than expected. Starting with the definition of essential entities, the task for Member States to define their essential entities proved out to be counterproductive in terms of leveling the playing field, as Member States designated essential units in different ways. [5]

Without unified criteria, Member States faced inconsistent implementations regarding incident thresholds, regulatory burdens, cooperation, and information sharing. This lack of standardization led to confusion about what constitutes as an essential entity, as well as resource limitations and unclear obligations. Additionally, achieving compliance was associated with operational costs, which many found

unfair, as one member state might designate a certain-sized hospital as an essential entity, while another state might not. [5]

3.1.2 Reporting and Penalties

Another noticeable shortcoming of the Directive concerned the vague criteria concerning the identification of an incident and the informal notification of an incident. In accordance with Article 14, the significance of the impact of an incident is determined by the number of users affected, the duration and the geographical spread with regard of the area affected by the incident [19, Art. 14]. Regarding the reporting obligation, the operators of essential services must notify the competent national authorities about significant incidents without undue delay and the report must include enough detail about the nature of the incident, measures taken and its potential consequences [20].

However, given the already varying designations of essential entities, the generality of the criteria left the identification up to interpretation. As a result, some states reported very few to no incidents, while studies indicated a different reality. In addition, communication between Member States remained low, and by 2018, when the Directive was already in force, only a few Member States had engaged in cross-border consultation on the alignment of regulatory requirements, i.e. on the criteria for the identification of material entities. [21, p. 14]

Regarding penalties for non-compliance, these were defined at the national level by each Member State. This led to significant variations in how penalties were applied across the EU. Some countries imposed very minimal penalties, while others set fines that were much higher. In some instances, no maximum penalty was set, resulting in full flexibility to the national authority. Eventually, this lead to weaker overall adherence to the directive's requirements. [21, p. 16]

To address these shortcomings and to keep up with the increased digitization

and evolving cybersecurity threat landscape, the directive was revised and updated. This effort was led by the European Commission, in collaboration with the European Parliament and the Council of the European Union resulting in the Directive on measures for a high common level of cybersecurity across the Union, known as the NIS2 Directive. [4]

3.2 NIS2 Directive

As reflected in Section 3.1, the initial Network and Information Systems Directive established the foundation for cyber preparedness and resilience across the European Union. However, its implementation revealed several challenges that limited its effectiveness in achieving a uniform level of cybersecurity across the Member States.

With the revised NIS2 Directive, the scope has been expanded to include additional sectors and entities, accompanied by clearer and stricter requirements. This expansion also acknowledges the importance of risk management and aligns with global standards by incorporating cybersecurity best practices and international frameworks. This approach aims to address the shortcomings of NIS Directive and establish a more resilient and effective cybersecurity framework across the EU, ensuring a stronger and more sustainable approach against evolving cyber threats. [22, Ch. 1]

By expanding and refining the scope of affected sectors with minimal room for interpretation, the NIS2 Directive addresses the inconsistencies seen under NIS1. This ensures that all Member States now follow the same guidelines, promoting fairness and reducing discrepancies in the application of cybersecurity measures across the EU. By introducing clearer enforcement mechanisms and stricter penalties for non-compliance, adherence and accountability can be more effectively tracked and addressed.

3.2.1 Objectives and Measures

As the main objective of the NIS2 Directive is to achieve a high common level of cybersecurity across the EU, greater involvement from Member States and stricter obligations are expected. To achieve this, the directive lays down four provisions to achieve this goal. [22, Art. 1]

National Cybersecurity Strategies and Authorities

The first provision states that Member States must adopt national cybersecurity strategies and establish competent authorities, cyber crisis management authorities, single points of contact, and computer security incident response teams (CSIRTs) to cohesively increase effectiveness and coordination regarding cybersecurity threats. As mentioned in Section 3.1.1, these establishments were also present in the initial NIS Directive. As a new addition, the NIS2 Directive defines the national cybersecurity strategy more holistically, with the scope extending to cybersecurity in general.

This includes defining strategic objectives and priorities, governance and risk management structures, and the means to achieve them rather than just specifying technical and operational measures concerning the security of network and information systems. In addition, the strategy should include a governance framework and policies to identify and address critical roles, assets, risks and vulnerabilities, and a plan which defines the necessary measures to enhance cybersecurity awareness and relevant procedures to support information sharing. [22, Art. 7]

While Member States are able to adopt and implement the strategies based on their national needs, the minimum requirements, such as policies regarding supply chain security, guides the member states towards a higher level of quality and resilience in their cybersecurity initiatives [5]. The strategy shall be notified to the Commission within three months of its adoption and has to be assessed and updated at least every five years. A Cooperation Group is also established to particularly aid

in reviewing the proposed strategies, advice and cooperate with the Member States with the support of CSIRTs network, EU-CyCLONe, and the Critical Entities Resilience Group. [22, Art. 7, 14]

Regarding the authorities, contacts and teams responsible for the implementation, coordination, prevention, response and recovery of cybersecurity efforts and the NIS2 Directive enforcement, these are to be clearly stated and informed to relevant parties to ensure effective monitoring and management of incidents, while also up keeping secure communication channels for internal and cross-border information sharing. [22, Art. 8–10]

Risk Management Measures and Reporting Obligations

The second provision consists of the required risk management measures and reporting obligations concerning the entities under the directive. As a baseline, the risk management measures must take into account the state-of-the-art practices present in international standards and have proportions relative to the degree of the entities exposure to risks, size, and impact on society and economy. With cooperation with Member States, the European Network and Information Security Agency (ENISA) is the responsible entity for creating advice and guidelines on technical areas, based on existing standards [22, Art. 25].

Minimum requirements for the measures include policies and tools for e.g. incident handling, business continuity, supply chain security, cryptography, vulnerability and asset management, cybersecurity training, and multi-factor authentication. In addition, independent and regular cybersecurity assessments are expected for evaluating the effectiveness of the measures [22, Art. 21]. The Cooperation Group in collaboration with ENISA act as the advisory entities and may carry out security risk assessments regarding critical ICT services, systems or product supply chains. [22, Art. 12]

While the initial NIS Directive's incident reporting obligations applied only to operators of essential services and digital service providers [19, Art. 14], the reporting obligations in the NIS2 Directive are broadened and concerns the defined essential and important entities. Whereas NIS Directive determined the incident's significance based on the number of users affected, duration, and geographic spread, NIS2 Directive specifies the severity of the incident based on a set threshold. The severity of an incident in NIS2 is determined by it's capability to cause severe operational disruption, financial loss, material or non-material damage. This also includes instances where these effects have already occurred. [22, Art. 23]

In the case of a significant incident, the entity is obliged to provide an early warning to the relevant CSIRT or competent authorities within 24 hours of becoming aware of the incident, including sufficient details about the incident. 72 hours after the initial notification, a more detailed report is expected, including updated information about the incident, its severity, impact and indicators of compromise. A final report is expected after a month of the submission of the detailed report or the resolution of the incident. This must include a detailed description of the incident, including its severity, impact, root cause, mitigation measures and cross-border impact if applicable. In addition, the entity is responsible of informing their clients and affected parties of the incident without delay. [22, Art. 23]

These obligations represent significant changes to the original directive. As noted in Section 3.1.2, the vagueness of the incident definition and reporting obligations may have contributed to the unrealistic volume of incident reports under the NIS Directive, but now with more detailed specifications, time limits, and further involvement of national and supervisory authorities faster reaction, stronger resilience and recovery is to be expected.

Information Sharing

The third provision concerns the rules and obligations on cybersecurity information sharing, emphasizing the establishment and utilization of channels for continuous exchange of information to raise awareness. This includes information related to cyber events and relevant recommendations for procedures and tools to avoid, detect and recover from cyberattacks. While this mainly concerns entities under the directive, other relevant entities are also able and encouraged to exchange information on a voluntary basis. [22, p. 23]

In addition to the notification obligation under Article 23, Member States must ensure that notifications can be voluntarily submitted to CSIRTs or competent authorities for incidents, cyber threats, and near misses. These notifications may be processed based on criticality and will not impose additional obligations for the entity had it not voluntarily submitted the notification, unless the notification meets the reporting obligations and reveals criminal negligence or breaches legislation.

Supervision and Enforcement Obligations

The fourth provision lays down supervisory and enforcement obligations. Under the initial NIS Directive Member States were obliged to individually determine the suitable penalties for infringements of the national provisions [19, Art. 21]. NIS2 Directive proposes significant changes to the infringement procedure with a uniform proceeding for the administrative fines, imposed for infringing the listed risk management measures in Article 21, the reporting obligations presented in Article 23 or for failing to comply with control and enforcement measures according to Article 32 or cooperate on information sharing and reporting requirements set out in Article 33.

For essential entities, the maximum fine reaches EUR 10 000 000 or 2% of total worldwide annual turnover, depending on whichever is higher. For important

entities, the maximum fine reaches EUR 7 000 000 or 1.4% of total worldwide annual turnover. As the fines are issued by the supervisory entities, Member States must ensure that the supervisory and enforcement measures can be carried out in an effective, proportional and dissuasive manner. [22, Art. 34]

The competent authorities recognized by Member States are responsible for the supervision based on a predefined criteria. For essential entities this includes on-site and off-site inspections, regular, targeted and unannounced security audits and requests for documentation, data access and evidence of implementation of cybersecurity policies. The enforcement powers allow the supervisors to impose warnings, binding instructions, fines, revoke certifications and designate a monitoring officer for a determined period to oversee compliance. Additionally, the criteria holds the legal representatives of essential entities personally liable. This means that individuals who have the authority to represent the entity and make decisions on its behalf can be held accountable. Failure to comply with NIS2 may be considered a breach of their duties as Article 20 also expresses that the management of an entity must be involved in the preparation and implementation of cybersecurity policies. [22, Art. 20, 32]

For important entities, the measures have an emphasis on ex-post supervision after evidence of non-compliance is identified, meaning that action is primarily conducted once there is suspicion or evidence indicating that the important entity is not in compliance. This includes posterior inspections and information requests, targeted security audits and proof of cybersecurity policy implementations, which are primarily paid by the audited entity. For important entities, warnings, fines, and conduct ceasing can also be imposed, but a dedicated monitoring officer is not assigned due to the lack of pro-active supervision. In accordance with Recital 133 and Article 20, competent authorities may impose suspensions or prohibitions on legal representatives in cases of infringement. However, such penalties must be pro-

portionate to the level of risk posed by the entity and for important entities, are not as stringent as those applied to essential entities. [22, Rec. 133, Art. 20, 33]. These key differences are summarized and presented in Table 3.1.

Table 3.1: Key differences between essential and important entities. Adapted from EU 2022/2555 [22].

Aspect	**Essential**	**Important**
Criticality	Disruption of services has serious consequences for public safety, health, and economic stability.	Disruption of services may cause significant harm, but it is less severe than that of essential entities.
Penalties	€10 million / 2% global turnover, with legal representatives potentially held directly liable	€7 million / 1.4% global turnover, with legal representatives held proportionally responsible.
Suspensions	Depending on the severity of an incident or infringement, services, certifications, authorizations and executive roles may be suspended until the deficiencies has been remedied.	Similar actions, but only after non-compliance has been identified through evidence or investigation.
Supervisory Powers	On-site inspections, off-site supervision, regular, targeted and ad-hoc security audits, access to documents, adequate information requests and evidence of compliance.	Focus on regular security audits and information requests, including access to data, documents, and evidence of cybersecurity measures, unless there is evidence, indication or information of non-compliance.
Enforcement Powers	Fines, warnings, binding instructions with time limits, designation of a monitoring officer, orders to cease conduct, rectify deficiencies in a specified period, and inform affected parties.	Similar actions, but proportional to the entity and primarily after evidence, indication or information of non-compliance emerges.

Commission Implementing Regulation (EU) 2024/2690

To support the Directive on measures for a high common level of cybersecurity across the Union, the European Commission published a specification on 17 October 2024, the requirements and rules for implementing Directive (EU) 2022/2555 called the Commission Implementing Regulation (EU) 2024/2690. This outlines the technical and methodological rules for cybersecurity risk management measures, making the requirements mandatory for affected entities.

In addition, the regulation further defines a significant incident, with the criteria of it being able to cause a direct financial loss exceeding €500,000 or 5% of global turnover, whichever is lower, reoccurs twice within 6 months or involves exfiltration of trade secrets, significant harm to health, or death. It also defines incidents for service providers like DNS, cloud, data centers, and trust services, based on extended downtime, extensive user impact, or compromised data confidentiality, integrity, or authenticity. [23]

Regarding the proposed measures, these are derived from European and international standards, such as ISO/IEC 27000 family, ETSI EN 319401 amd CEN/TS 18026:2024. It covers various areas, such as risk management, incident response and data protection, with specific requirements like logical separation of administrative systems, asset classification with levels, multi-factor authentication, and cryptographic methods for key management. ENISA is further developing technical guidance to provide additional explanations of these requirements, as well as mapping them to European and international standards. [23], [24]

3.2.2 Scope

In article 1 of the initial NIS Directive, essential service providers and digital service providers are identified as the key groups to which the directive applies to [19, Art. 1]. These are entities that provide vital services with societal, economic, and digital

importance. However, since member states were allowed to define these groups and organizations further, there was significant variation in which organizations were required to comply.

With NIS2, the scope of the directive is extensively expanded. With a classification based on risk level and impact of disruption, entities to which the directive applies are divided into **Essential** and **Important**. While both essential and important entities are of significant societal and economic importance, essential entities are considered more vital for stability, whereas important entities have a lower level of criticality in comparison. In addition to the previously established key groups, the directive includes medium-sized enterprises, as well as the entities presented in Table 3.2, which are included regardless of their size.

The criticality of entities is evaluated primarily by their size and derived from the commission's recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. Large entities are defined as organizations with more than 250 employees or an annual revenue exceeding €50 million. Medium-sized entities refer to organizations with 50-249 employees or annual revenue between €10-50 million and entities smaller than this are listed as small entities. [25]

Table 3.2: Entities included regardless of their size. Adapted from EU 2022/2555, [22, Art. 2] and NCSC NIS2 Entities [26].

Sector	**Large**	**Medium**	**Small**
Providers of public electronic communications networks/services	Essential	Essential	Important
Trust service providers	Essential	Essential	Essential
Top-level domain name registries	Essential	Essential	Essential
Domain name system service providers	Essential	Essential	Essential
Sole providers of essential services in a Member State	Essential	Essential	Essential
Entities whose disruption impacts public safety, security, or health	Essential	Essential	Essential
Entities whose disruption causes systemic risk with cross-border impact	Essential	Essential	Essential
Entities critical at national/regional levels for specific sectors or interdependent services	Essential	Essential	Essential
Public administration entities of central governments	Essential	Essential	Essential
Public administration entities of regional or local governments	Important	Important	Important
Critical entities under Directive (EU) 2022/2557	Essential	Essential	Essential
Educational institutions with critical research activities	Important*		
Domain name registration service providers	Essential	Essential	Essential

* Unless activities are tied to critical infrastructure or services.

Essential sectors of high criticality include sectors whose criticality is defined by basic criteria based on the previous definition, whereby large entities are considered essential, medium entities as important, and small units excluded from the scope. Other critical sectors are considered important and included in the scope if they exceed the criteria of small and micro entities, meaning they have more than 50 employees or annual revenue exceeding €10 million. These are presented in Table 3.3.

Table 3.3: Essential sectors of high criticality and other critical sectors. Adapted from EU 2022/2555, [22, Ann. 1, 2].

Essential sectors of high criticality	**Other critical sectors**
Energy	Postal and courier service
Transport	Waste management
Banking	Chemical manufacture, production and distribution
Financial market infrastructures	Food production, processing and distribution
Health	Manufacturing
Drinking water	Digital providers
Waste water	Research
Digital infrastructure	
ICT service management	

In conclusion, the NIS2 Directive aims at rectifying the shortcomings of its predecessor by listing the concerned entities and their responsibilities with less room for interpretation. With a systematic classification process and clearer obligations set, diversion in the selected critical entities between Member States can be mitigated, resulting in a more unified structure and more coherent information sharing and policy-making. As the supervisory and enforcement powers permit the competent authorities to issue substantial fines and effectively monitor the entities' compliance, entities under the directive are compelled to meet these requirements and independently take action into increasing their cyber resilience.

3.2.3 Integration of the NIS2 Directive into Finland's National Legislation

Although the applicable legislation in Finland regarding the NIS2 Directive has not yet been implemented at the time of writing, the draft recommendation for NIS supervisory authorities has been published.

This publication includes twelve essential cybersecurity risk management measure categories, which are adapted from the upcoming legislation being prepared by the Ministry of Transport and Communications and designed to ensure compliance with the NIS2 Directive. The measures align with both the proposed amendments to the upcoming Cybersecurity Risk Management Act (HE 57/2024) and updates to the Act on Information Management in Public Administration (906/2019), highlighting key practices that organizations must adopt to effectively manage cybersecurity risks across communication networks and information systems. [27], [28]

The twelve cybersecurity risk management measure categories are presented in Table 3.4.

Table 3.4: Cybersecurity Risk Management Measures and Sections of HE 57/2024 Art. 9 [28]

Article 9	**Measure**
Section 1	Risk Management Policies
Section 2	Network and System Security
Section 3	Secure Development and Vulnerability Management
Section 4	Supply Chain Resilience
Section 5	Asset Security
Section 6	Staff Training
Section 7	Access Control
Section 8	Encryption and Secure Communications
Section 9	Anomaly Detection
Section 10	Business Continuity
Section 11	Basic Security Practices
Section 12	Physical Security

4 Cybersecurity Maturity and Frameworks

4.1 Definition and Scope

Cybersecurity refers to the protection of cyberspace – an environment resulting from the interaction of people, software, and services on the Internet – through the means of technology, policies, and practices [29]. While its definition has evolved and varied over time, the focus on the preservation of confidentiality, integrity, and availability of information remains as its core. [30], [31]

Maturity, in the context of assessment, refers to the demonstrable evolution from an initial state to a desired state. One definition for maturity is the state of completeness, readiness, or perfectness, and it can be reflected in three ways: process-maturity, which indicates how defined, managed, and effective a process is; object-maturity, which indicates the sophistication of a product; and people-capability, which refers to the workforce's ability to create knowledge and improve proficiency. [32]

Incorporating these perspectives, a maturity model is comprised of characteristics, attributes, indicators, or patterns representing capability and progression [33]. It evaluates the comprehensiveness and manageability of processes, the effectiveness of objects and tools in meeting their objectives, and the workforce's capability to

foster understanding in their operations, resulting in the production of knowledge.

Cybersecurity maturity models provide a framework to assess an entity's ability to manage and respond to cybersecurity risks effectively. By analyzing the processes, practices, and controls related to the protection of assets, systems, data, and people, a maturity level can be determined indicating the entity's ability to predict, prevent, detect, and respond to threats. Serving as a benchmark, cybersecurity maturity models guide entities in identifying their current level of maturity and developing a pathway for improvement. Through an ongoing and systematic process, entities are able to gain insights into their risk exposure, strengths, and weaknesses while facilitating the implementation of necessary controls to strengthen their cybersecurity posture.

4.2 Use Cases and Key Frameworks

With the growing cyber awareness and attention to cybersecurity management by organizations, governmental institutions, and investors, as highlighted in 2.1, the importance of information security assurance and certification has increased. Several sectors are already required to maintain specific cybersecurity certifications as a condition for operations. Entities under the NIS2 Directive are also expected to address globally recognized standards in their risk-management measures and protection of systems [22, Rec. 79]. Acknowledged and addressed in the NIS2 Directive, alongside ENISA's 2024 cybersecurity control recommendations [3, Ann. B], the most prominent standards for cybersecurity management, certification, and best practices are provided by the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST).

4.2.1 ISO/IEC 27000 Family

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are two prominent organizations that develop global standards to support consistent and high-quality management practices across industries. In collaboration, they have developed the ISO/IEC 27000 family, which includes several standards aimed at supporting comprehensive information security management across multiple domains.

ISO/IEC 27001 is an international standard focused on Information Security Management Systems (ISMS). As the key standard in the family, it outlines the requirements for establishing, implementing, maintaining, and continuously improving an ISMS [29]. This standard emphasizes a risk-based approach, requiring organizations to assess their information security risks considering confidentiality, integrity, and availability of information and implementation of controls to address them [34]. In total, ISO/IEC 27001 includes 144 different controls, each addressing risk management measures with varying emphasis. Of these controls, fifteen in total, focus on physical and environmental security, which is one of its core control areas. [35].

Regarding cybersecurity maturity assessment, the ISO/IEC 27004 standard provides guidelines on monitoring, measuring, analyzing and evaluating the effectiveness of the Information Security Management Systems (ISMS), which refers to the overall systems and processes that organizations utilize to manage information security risks. It utilizes the ISO/IEC 27001 as the basis for best recognized practices and provides tools to fulfill the requirements of ISO/IEC 27001. [36]

While not formally categorizing maturity levels, ISO/IEC 27004's principles align closely with the concept of measuring an organization's information security maturity. This is achieved through the assessment of an information security management system, with its resilience being reviewed through monitoring, measurement, analysis, and evaluation [36].

4.2.2 NIST Cybesecurity Framework

The NIST Cybersecurity Framework (NIST CSF) was created by the National Institute of Standards and Technology to help organizations manage cybersecurity risks. While it is mandatory for U.S federal contractors, it is increasingly being adopted by private companies globally to manage and reduce cybersecurity risks. With the 2024 revision, NIST CSF 2.0 expands the focus on governance and supply chain risk management with increased support for smaller organizations.It consists of six core functions: Govern, Identify, Protect, Detect, Respond, and Recover, each reflecting an important component of cybersecurity. These are divided into categories, which are further divided into subcategories representing practices that are considered exemplary. [37].

Considering maturity assessment, NIST CSF includes the concept of CSF Profiles and Tiers. Based on the core functions outcomes, Profiles determine the current and target cybersecurity postures. These are used to understand, tailor, assess, prioritize and communicate the organization's state and takes into consideration its objectives, expectations, landscape, and requirements. Tiers, on the other hand, characterize the profiles with a rating, ranging from informal to adaptive (1-4). These act as benchmarks to assess and monitor progress, while also providing an efficient way to communicate current and target levels to relevant stakeholders. [37].

While training programs are available to become a certified lead implementer of the framework, the framework itself is not certifiable in the way as ISO/IEC 27001 is. Instead, it serves as a flexible, high-level guide for risk management and cybersecurity strategies, allowing it to be tailored to the organization's needs and size. With a comprehensible risk language, it is efficient in bridging technical and non-technical stakeholders by promoting clear communication, aligning cybersecurity objectives with business goals, and involving all levels of the organization in decision making. [37], [38]

4.2.3 Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (C2M2) is a framework developed by the U.S. Department of Energy to help organizations assess their cybersecurity capabilities. It consists of 10 critical domains, including risk management, asset management, and incident response. Each domain includes specific practices that organizations can implement to improve their cybersecurity posture. C2M2 is particularly useful for organizations looking to establish a clear understanding of their current cybersecurity capabilities and identify areas for improvement. [39], [40]

Following a similar tier approach as NIST CSF, C2M2 defines progression from initial ad hoc practices (Level 1) to adaptive and continuously improving security practices (Level 5). For the self-evaluation process, organizations are expected to evaluate and input their implementation levels for the presented practices, which generate reports summarizing cybersecurity gaps and help in developing remediation strategies. [39]

In collaboration with the NIST National Cybersecurity Center of Excellence, bidirectional mappings have been developed to align C2M2 with the NIST Cybersecurity Framework (C2M2-to-CSF and CSF-to-C2M2) and are available for the public [41]. This demonstrates that C2M2 also serves as a complementary tool, effectively integrating and supporting other cybersecurity frameworks. In addition, since it isn't restricted by licenses, organizations can freely use, adapt, and implement C2M2 publicly, and it is used as a base for several other models, such as Kybermittari.

5 Methodology and Selection

The NIS2 Directive recognizes the need for stronger cybersecurity risk management, requiring organizations to implement technical, operational, and organizational measures to prevent and mitigate cyber risks. As stated in Article 21 of the NIS2 Directive [22] (Art. 21), the measures "shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents". The article's listed measures include the assessment of policies and procedures to evaluate the effectiveness of cybersecurity risk-management measures. This aligns with the need for conducting cybersecurity maturity assessments, a key focus of this thesis, which evaluates the organization's progress and readiness in managing cyber threats.

To evaluate potential hazards, it is essential to conduct a comprehensive assessment of the organization's most valuable assets and the effectiveness of existing measures in terms of cybersecurity. As the entity of this assessment prepares to take steps to meet NIS2 compliance, a thorough analysis of the current situation is required, and this will be conducted in the form of a Cybersecurity Maturity Assessment. To find the appropriate tool for this assessment, a reflection on the sector-specific requirements will be considered. Also, the assessment of the applicability of the existing solutions in relation to NIS2, the manufacturing industry, and Finnish law will be covered.

5.1 Scope of Methodology

The scope of this assessment is restricted to evaluating the cybersecurity maturity of a local production network, which operates in a controlled and isolated environment. Managed by the local IT department, this network is integral to the company's daily operations. Given its role, the network is separated from the broader organizational network to reduce risks, improve security, and to have extensive control of its components.

Due to its critical nature, the responsibilities of the IT infrastructure team are paramount in maintaining the integrity, resilience, and security of this network. The team is tasked with implementing and enforcing security measures, conducting regular maintenance, monitoring, and ensuring compliance with relevant standards and regulations. This crucial role will be assessed as part of the maturity evaluation process.

Since the primary purpose of the selected tools is to assess cybersecurity maturity levels, it's essential that the tools include a clear and structured criteria which are applicable across different cybersecurity domains. These should also enable objective and systematic inspection, and consistent basis for evaluating the effectiveness of the implemented measures.

The initial evaluation criteria must also account for the organization's size and industry-specific needs. Given that the organization operates on a large scale, assessment frameworks designed for small or medium-sized enterprises (SMEs) may lack the depth and scalability required to comprehensively assess the level of cybersecurity maturity across areas such as risk management, incident response, and business continuity.

Given the company's role in manufacturing, any selected frameworks must also address the sector-specific needs in areas like data protection, regulatory compliance, and supply chain security. These aspects are critical in ensuring the company's

operations meet both legal requirements and best practices recognized.

Manufacturing companies are advised and demanded to follow certain industry standards, such as the rules for good working practice (GxP) including practices for manufacturing (GMP), distribution (GPD), and international certifications e.g. ISO 17025 and 13485 which outline the requirements for maintaining product quality, data integrity and safety in device production and testing [42], [43].

Taking these pre-established practices and certificates into account, they can provide assurance that fundamental operations are in order and assist in the quantitative analysis part of the assessment.

While the existing certifications may help in verifying the existence of required measures and elements, the frameworks should assess the depth and maturity of implementation, examining whether the cybersecurity measures form a cohesive and holistic posture rather than a checklist of isolated controls. This is crucial to ensure that the company's approach to cybersecurity is not only compliant with the NIS2 Directive but is also robust, adaptive, and integrated into day-to-day operations.

5.2 Evaluation and Scoring

As the maturity assessment is to be carried out to support compliance with the NIS2 Directive in Finland, the essential elements and priorities of the NIS2 Directive are recognized and used as the key evaluation criteria in deciding which frameworks to use. In accordance with Section 3.2.3, the twelve presented risk management measures can be utilized in the evaluation.

With the foundational measures established, the key sub-areas for maturity assessments can be outlined, allowing the publication to serve as a basis for evaluating the maturity model in relation to the measures presented. The measures overlap between categories, but generally can be summarized and placed into the following three security measure categories (*):

a. **Operational and System Security:** Daily technical controls safeguarding IT/OT infrastructure, including asset management, access control, and threat mitigation.

b. **Resilience and Continuity:** Preparedness for disruptions through incident response, recovery planning, and maintaining business operations.

c. **Risk Management and Governance:** Strategic oversight and policy frameworks for comprehensive risk assessment, management, and compliance.

These were categorized based on their primary focus and nature of their objectives. Targeting distinct areas of cybersecurity, these three categories emphasize measures for day-to-day security, readiness for disruptions and recovery and strategic management promoting long-term resilience and government. The measures and their respective categories are presented in Table 5.1.

Table 5.1: Risk Management Measures, Definitions and Categories. Adapted from the Finnish Transport and Communications Agency, 2024 [27].

Risk Management Measures	**Definition**	*****
Risk Management Policies	Policies to manage cybersecurity risks and assess risk management effectiveness.	c
Network and System Security	Policies for securing communication networks and information systems.	a
Secure Development and Vulnerability Management:	Security in acquisition, development, and vulnerability handling.	a
Supply Chain Resilience	Ensuring product and service quality, assessing cybersecurity risks, and risk management in the supply chain.	b/c
Asset Security	Managing and identifying assets critical to cybersecurity.	a
Staff Training	Cybersecurity-focused staff security and training measures.	c
Access Control	Procedures for access control and authentication.	a
Encryption and Secure Communications	Policies for encryption and secure communication.	a
Anomaly Detection	Systems to detect and address anomalies, ensuring safety and security.	a
Business Continuity	Backup, recovery, and crisis management planning.	b
Basic Security Practices	Operational and data security practices for protecting information.	a
Physical Security	Measures for the physical security of networks, systems, and supporting infrastructure.	b

The scoring system for evaluating the applicability of the frameworks is inspired by the tiered approach common in established cybersecurity maturity models, such as the Cybersecurity Capability Maturity Model (C2M2) [39]. Adapting the maturity indicator levels from C2M2, the evaluation follows these criteria:

- **Score 0 (No coverage):** The category is not addressed in the framework
- **Score 1 (Minimal mentions):** The framework recognizes the category, but in a less detailed and general way
- **Score 2 (Comprehensive measures):** The framework provides a comprehensive overview of the category, covering the main aspects
- **Score 3 (Best practices):** The framework highlights the category's relevance with detailed measures aligned with recognized best practices

This approach reflects the increasing sophistication in practices and relevance regarding the topic. The twelve security measures addressed are categorized under the presented security categories: *Risk Management and Governance, Operational and System Security, and Resilience and Continuity.* These will be individually evaluated based on the framework's focus and relevance on the corresponding region. Since adapting the framework to fit local requirements and the NIS2 Directive is a crucial part of the assessment, *Alignment with NIS2 or other relevant regulation* will be added as an additional evaluation category.

With the suitable categories of importance identified, each section is evaluated and assigned a score based on the previously defined evaluation criteria. The scoring and security measure categories are further detailed and cross-summarized in Table 5.2.

Table 5.2: Categories and Scoring Criteria

Category	Score 0	Score 1	Score 2	Score 3
Risk Management and Governance	No criteria/tools for assessing risk management maturity.	Lacks depth or detail in governance practices and assessment of maturity levels.	Clear and detailed criteria, including risk assessments, policies and leadership oversight.	Advanced, risk-based, and best-practice criteria, emphasizing continuous improvement [44].
Operational and System Security	No criteria or tools for evaluation.	Covers only basic measures.	Criteria includes vulnerability management, incident response and security practices.	Criteria emphasizes proactive, real-time monitoring and security automation [45].
Resilience and Continuity	No criteria for evaluating disaster recovery or resilience.	Minimal criteria for continuity and recovery plans, lacking regular inspection.	Clear criteria for business continuity and disaster recovery.	Advanced, detailed criteria with regular testing, continuous improvement, and recovery capability [46](Art. 11).
Alignment with NIS2 or other relevant regulation	No alignment with NIS2 or relevant regulations.	Acknowledged by NIS2 or other regulations, but unclear involvement.	Overview of alignment with NIS2 and relevant regulations, but lacks detail.	Clearly describes compliance with NIS2 and relevant legislation.

5.3 Maturity Model Framework Selection

To determine the suitable frameworks to be utilized for the maturity assessment, it is essential to identify the foundation of the practices outlined in the NIS2 Directive. While the NIS2 Directive avoids specifying individual frameworks or standards, it leaves EU Member States the flexibility to emphasize and adapt these tools according to their needs, particularly concerning critical infrastructure and organizational practices.

In alignment with this flexibility, the National Cyber Security Centre of Finland (Traficom) has examined the NIS2 Directive alongside the national draft of

the Finnish government's proposal to propose the prementioned draft recommendation for NIS supervisory authorities. The drafts development has also included collaboration with EU Member States and the European Union Agency for Cybersecurity (ENISA), which has been acknowledged as an essential factor in determining the best EU-wide practices, significantly affecting the requirements outlined in the NIS2 directive [47].

This preparatory work has also involved adaptation of established information security standards and assessment tools, including ISO/IEC 27001, IEC 62443, the NIST Cybersecurity Framework (NIST CSF), Julkri and Kybermittari. [27]

With specific frameworks identified, each will be initially inspected based on their suitability and comprehensiveness. Those meeting the initial criteria will be added to the evaluation pool and based on the results, utilized to complement other frameworks if necessary. Additionally, several globally recognized frameworks have been added for review, and presented in Table 5.3, along with relevant remarks and whether included to the evaluation pool.

Table 5.3: Overview of Cybersecurity Maturity Frameworks for Initial Screening

Framework	Description	Reasoning	Incl.	Src.
NIST Cyber Security Framework - CSF 2.0	Provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks.	Provides a comprehensive and globally recognized framework, aligning well with the NIS2 Directive's risk-based approach.	Yes	[37]
National Cybersecurity Assessment Framework - NCAF, ENISA	For measuring the maturity level of the cybersecurity capabilities of the Member States to support them in conducting an evaluation of their national cybersecurity capability.	Focuses on national level assessments, which may not be applicable to the private organization of this assessment.	No	[48]
Security Incident Management Maturity Model – SIM3, ENISA	For measuring the maturity of Computer Security Incident Response Teams (CSIRTs) considering relevant EU policies.	Focuses on the maturity assessment regarding CSIRTs. Not applicable for this assessment.	No	[49]
Cybersecurity Maturity Assessment for SMEs - ENISA	For small and medium sized businesses to assess and enhance their cybersecurity maturity level.	Focuses on SMEs, which falls outside the scope of critical or important industries.	No	[50]
ISO/IEC 27000 family - Information security management	For implementing and improving an Information Security Management System (ISMS) focused on data protection and risk management.	Provides a comprehensive and globally recognized framework for managing and evaluating cybersecurity posture.	Yes	[29]
Cybersecurity Capability Maturity Model - C2M2	For evaluating cybersecurity capabilities and assessing cybersecurity capabilities across IT and OT environments.	Provides a structured approach and is suited for organizations with complex and critical infrastructures.	Yes	[39]
Kybermittari - Cybermeter	A tool developed by National Cyber Security Centre (NCSC-FI) to control cyber threats and assess critical functions, processes, and dependencies.	Focuses on Finnish organizations for assessing cybersecurity maturity in alignment with best practices and Finnish legislation.	Yes	[51]
Assessment criteria for information security in public administration - Julkri	A national tool to support public administrations in assessing and improving information security.	The framework is targeted at public administrations, making it unsuitable for private organizations.	No	[52]
CIS Controls Maturity Model v8 & CMMC	A mapping tool to assess cybersecurity posture in relation to CMMC requirements.	Strong emphasis on operational controls and risk management but lacks scalability and emphasis on continuous improvement and metrics.	No	[53]

Framework	Description	Reasoning	Incl.	Src.
Zero Trust Maturity Model	A Maturity model based on the foundations of zero trust with an emphasis on access controls, data protection and timelessness.	Focuses on access control and encryption. Has limited coverage regarding e.g. risk management policies, supply chain security and asset security management.	No	[54]
COBIT 2019	A governance framework for IT and business alignment, which includes evaluating IT governance and management processes, including cybersecurity, through maturity assessments.	Does not directly address specific cybersecurity maturity criteria and places too much emphasis on governance.	No	[55]
Microsoft Sentinel: Cybersecurity Maturity Model Certification (CMMC) 2.0 Solution	Helps organizations align with CMMC 2.0 compliance by providing enhanced tools for monitoring, assessments, and alerting.	Focuses on reaching compliance with the CMMC 2.0 framework and strong emphasis on environments utilizing Microsoft products.	No	[56]
IBM Security Framework	Provides a reference model for essential security domains with security controls representing maturity levels within the domains.	Emphasis on providing best practices and guidance for securing environments. A vendor-centric solution with minimal focus on maturity assessment.	No	[57]

5.3.1 Evaluation

From the frameworks identified in the initial screening and listed in Table 5.3, a total of four frameworks were identified as suitable for the in-depth evaluation phase, NIST CSF 2.0, ISO/IEC 27000 Family, C2M2, and Kybermittari. These were selected based on the pre-established alignment with the objectives of this assessment: relevance to the cybersecurity maturity requirements of the NIS2 Directive, compatibility with industry standards applicable to manufacturing, and potential to complement other frameworks.

NIST CSF 2.0

NIST CSF 2.0 provides a flexible, risk-based approach to cybersecurity by emphasizing risk management, continuous improvement, and strategic governance. While it aligns with global standards and is recognized by the National Cyber Security

Centre of Finland, its direct applicability to evaluating NIS2 compliance is limited, requiring additional alignment efforts and external consideration of the Finnish NIS2 implementation (HE 57/2024). These results are presented in Table 5.4.

Table 5.4: NIST CSF 2.0 Evaluation [37]

Risk Management Measures	**Description**	**Score**
Risk Management and Governance	Core functions revolve around the development of risk management strategies and establishment of risk tolerance. Provides advanced, risk-based, and strategic governance criteria with an emphasis on continuous improvement.	3
Operational and System Security	Criteria is comprehensive and advanced, focusing on proactive defense measures, security automation, and real-time monitoring.	3
Resilience and Continuity	Provides advanced, detailed resilience and continuity criteria, emphasizing recovery testing, continuous improvement, and preparedness for disruptions.	3
Alignment with NIS2 Compliance Requirements or other relevant regulation.	Globally recognized and acknowledged by the National Cyber Security Centre of Finland [58] but lacks detailed coverage and alignment with NIS2	2

ISO/IEC 27000 Family

As elaborated in Section 4.2.1, ISO/IEC 27001 and 27004 have an emphasis on continuous improvement through regular audits and management reviews that let organizations monitor their progress and maturity over time. However, its prescriptive nature may make it less flexible [59]. Additionally, while the ISO 27000 family offers extensive guidance on best practices, cybersecurity maturity assessments, and methods for monitoring and evaluating information security, it lacks a streamlined framework for practical implementation. Its utilization requires extensive self-study, design, and facilitation to apply the standards effectively in an organization. The evaluation is presented on Table 5.5.

Table 5.5: ISO/IEC 2700 Family Evaluation [34], [60]

Risk Management Measures	**Description**	**Score**
Risk Management and Governance	Clear guidelines for risk assessment, defining policies, and establishing leadership oversight. ISO 27004's focus is on enhancing IT governance and provides tools for measuring effectiveness of risk management practices, while promoting continous improvement.	3
Operational and System Security	Provides exemplary practices for vulnerability management and incident response (ISO/IEC 27001 & 27002).In the 2022 revision, real-time monitoring and security automation has been included, but with ISO 27004's revision being in preparation, suitable tools for evaluation are missing.	2
Resilience and Continuity	Business continuity and disaster recovery are noted in the controls, but the focus developing an ISMS limits the criteria for resilience, testing and continuous improvement. May fall short in addressing recovery needs for production systems	2
Alignment with NIS2 Compliance Requirements or other relevant regulation	Aligns with NIS2's regulatory goals, including data protection, risk management and incident response, but falls short in incident reporting. Its presence is acknowledged in the Directive	2

C2M2 & Kybermittari

Kybermittari, developed in Finland, combines elements from various frameworks, including NIST CSF and C2M2 while addressing specific needs within the Finnish context. As it has been developed by Traficom to comply with Finnish laws and regulations, it incorporates national requirements and aligns with best practices recognized internationally. [27], [51]

It offers a structured approach for organizations to assess their cybersecurity maturity and develop improvement plans based on a holistic view of their capabilities. Kybermittari distinguishes itself by integrating aspects of organizational culture, employee awareness, and the importance of continuous improvement into its maturity assessment.

Kybermittari utilizes directly the practices present in C2M2, with the addition of a CRITICAL sector. C2M2 is a framework developed by the U.S. Department of Energy to help organizations assess their cybersecurity capabilities. It consists of several domains, including risk management, asset management, and incident response. Each domain includes specific practices that organizations can implement to improve their cybersecurity posture. As a notable difference, C2M2 requires that all lower level practices must be achieved for a higher maturity level, while Kybermittari requires that the majority of the practices in the current level are accomplished. [39], [40] The results of the evaluation are presented in Table 5.6.

Table 5.6: Kybermittari and C2M2 Evaluation [40], [51]

Risk Management Measures	Description	Score
Risk Management and Governance	Focus revolves around risk management and governance. Clear, flexible, and structured approach for evaluating organizational readiness to manage cybersecurity risks. May have limited depth for organizations with already mature governance and risk management practices in place.	3
Operational and System Security	Provides tools and benchmarks for evaluating operational security measures on a progressive scale. Targets are based on best practices.	3
Resilience and Continuity	Highlights business continuity and resilence measures, but limited in providing advanced and detailed metrics for resilience and continuity practices for complex organizations.	2
Alignment with NIS2 Compliance Requirements or other relevant regulation	Aligns with NIS2's regulatory goals thoroughly, as Kybermittari is purpose-built for achieving the NIS2 risk management requirements.	3

5.4 Conclusion

When comparing these maturity models, we see that while NIST and ISO/IEC 27001 provide solid frameworks for assessing cybersecurity maturity, they may not provide the comprehensive and localized approach that Kybermittari offers. Developed by Finnish experts and authorities, Kybermittari fills these gaps by addressing both technical and organizational aspects of cybersecurity, making it especially suitable for conducting a cybersecurity maturity assessment within the Finnish context.

In selecting a maturity model framework for the assessment, the analysis of NIST CSF 2.0, ISO/IEC 27001, C2M2, and Kybermittari highlights their respective strengths and limitations. Kybermittari's comprehensive nature, which incorporates key elements from the other frameworks while addressing their shortcomings, positions it as a fitting choice for the maturity assessment in this thesis. This, in addition that it has been utilized in the proposition for NIS Supervisory Authorities to monitor cybersecurity risk management measures under the NIS2 Directive's

monitoring measures [27], further solidifies its relevance and alignment with current Finnish cybersecurity requirements.

6 Assessment and Results

This chapter describes the process design, implementation, and results of the assessment. Kybermittari is utilized as a cybersecurity maturity model to support the evaluation of the processes and lays the groundwork for identifying the areas of development.

6.1 Process Overview

6.1.1 Objectives and Context

In the beginning of the assessment, an introductory presentation was held in order to explain in more detail the focus and objectives of the assessment. This included an explanation of what was to be done, the reason for it, and how it is done. The objective of assessing the current state of cybersecurity of the manufacturing network and identifying areas of improvement remained at focus, resulting in a detailed analysis that will help identify measures to improve resilience and compliance with the NIS2 Directive. The Directive highlights the strengthening of cybersecurity risk management measures, and this can be approached with an iterative process of evaluating the current status of processes, defining the steps for improvement, and reproducing the assessment. With the help of the Kybermittari-tool, a systematic approach can be achieved with clearly defined criteria for quality and efficiency of practices.

Although the obligations of the NIS2 Directive had not been transposed into national law at the time of the evaluation, proactive measures are expected of important and essential entities under the Directive and with the utilization of the draft recommendation, the NIS2 Directive and the Commission Implementing Regulation a preliminary understanding of the requirements can be formed.

In conclusion, the objective of the assessment is to identify critical functions regarding the subject of the evaluation and thoroughly address and evaluate their implementation defined by the sections of Kybermittari, consisting of the following sections:

- Critical Service Protection (CRITICAL)
- Change, and Configuration Management (ASSET)
- Threat and Vulnerability Management (THREAT)
- Risk Management (RISK)
- Identity and Access Management (ACCESS)
- Situational Awareness (SITUATION)
- Event and Incident Response, Continuity of Operations (RESPONSE)
- Third-Party Risk Management (THIRD-PARTIES)
- Workforce Management (WORKFORCE)
- Cybersecurity Architecture (ARCHITECTURE)
- Cybersecurity Program Management (PROGRAM)

The grade for each practice is given after a mutual agreement has been achieved, meaning that time-consuming and controversial topics are left for further evaluation, but with the intention of completing the started section during a session.

6.1.2 Roles and Responsibilities

As the evaluation is conducted internally, the members of the assessment team are formed from the people responsible for the operations of the manufacturing IT infrastructure. The team includes key personnel with expertise in operations, management, and cybersecurity, including the team's direct leader. With a team size of four, the key responsibilities can be conveniently distributed between the participants.

The facilitator of the assessment holds the responsibility of the preparation, implementation, and handling of the evaluation results. This also includes the demonstration of the initial assessment plan to the participants, managing the evaluation tool, and coordinating operations, including time management. The facilitator is also responsible for neutrality during the assessment, ensuring that the evaluation results remain objective, and in the case of disagreements, determines the suitable action for settlements and consensus.

The organizer of the assessment is responsible for the conditions of the evaluation, the availability of necessary resources and tools, while also promoting long-term commitment and cybersecurity development in the organization.

The remaining responsibilities are carried out by the participants in an expert role. Participating in the assessment from a business, cybersecurity, and risk management perspective, they are able to provide expert insight into the current state of the organization, while also supporting analysis of the results and the identification of improvable actions. Although the responsibilities in practice have an overlapping nature, the establishment of roles is advisable to ensure accountability, clarity, and effective collaboration within the team, while also promoting commitment to the process.

6.1.3 Tools and Methods

Kybermittari version 2.1 serves as the main tool of the assessment, providing the framework for guiding and enhancing the evaluation process. Developed by the National Cyber Security Centre Finland and tailored for Finnish organizations, it incorporates objectives derived from NIST CSF with the focus of assessing the level of organizations' cyber risk identification, protection, detection, response, and recovery.

Using the C2M2 framework as the foundation, Kybermittari is comprised of 11 sections, 46 objectives, and 383 individual practices, which are assessed as implemented on a score scale of 0-4, with the following levels: not answered, not implemented or unknown, partially implemented, mostly implemented, and fully implemented. Implemented measures represent a score of 3 or 4, while not implemented measures correspond to a score of 0-2. A section consists of three to six relevant objectives, each having approximately eight practices that reflect cybersecurity best practices.

The practices are organized in a hierarchical manner, representing increasingly demanding and advanced processes. Divided into 3 levels, the first level of the objective represents occasional commitment and requires all of the practices to reach a minimum score of 3 to obtain a maturity level of 1. Advancing to level 2, the practices become more documented, regular, and require over 50% of the current level's practices to reach the minimum score of 3 for a maturity level of 2. Level 3 represents a risk-based implementation with organisation-wide operation models. Similarly, over 50% of the practices are required for a maturity level of 3.

In order to proceed to the next level, the requirements of the previous level must be met. If the requirements are not sufficiently met, it remains crucial that the following practices are also evaluated, as they are utilized in the generated final reports and analyses produced. The total maturity level of a section is based on the

lowest score present in the objectives.

For communication and information sharing, Microsoft Teams was utilized to support the assessment, including a file drive for meeting minutes and a copy of the master version of the Kybermittari Excel-file.

6.2 Facilitation and Challenges

After a mutual understanding of the objectives, roles, and the usage of the tool was achieved, a weekly meeting was set in place. For each meeting, the sectors of evaluation were selected beforehand, and depending on the scope, one or two sectors were selected for self-evaluation on a copy of Kybermittari. Primarily, these were selected in the order defined by the tool or based on their length and context. Sections that were deemed complex, such as the CRITICAL-section, were left for joint evaluation. In order to remain neutral, the evaluation results carried out by the members weren't revealed until reaching the discussion phase on the implementation of the individual practices.

By systematically proceeding in the evaluation of each practice, the results of the two assessment groups were introduced, and depending on their similarity, the results were inserted in the master version of the tool. In the case of a similar result, the evaluation score was directly applied, while if the results were mixed, an opportunity was given to defend the reasoning behind the score.

Due to time constraints, each practice couldn't be individually documented ,and in most cases, could be outlined from the context. As the evaluation was aimed for internal use, the documentation in the form of comments was principally applied only for practices receiving a score of 2 (partially implemented). These were considered as areas for future improvements that could benefit from additional clarification. The practices that generated discussion or were considered significant were also commented on for future utilization of the results. If agreement could not be reached

on a practice, it was left until the end of the session for a final verdict.

At the end of each session, attendance, time spent, covered sections, remarks, and next week's objectives were documented in the meeting notes. In the absence of an evaluator, the evaluation scores with clarifying comments were shared with the facilitator and taken into account when completing the results. These results were to be reviewed at the beginning of the next session, when the absent person has the opportunity to defend their arguments.

With the intent of completing the assessment before the year's change, a longer session was reserved for the final session. In the final session, the remaining sectors were collectively evaluated and the completed evaluations reviewed for potential flaws. After a general overview of the results, the process and next steps were discussed. In addition, the preliminary agenda and date of the results presentation meeting were also set. Figure 6.1 presents the progression of the assessment.

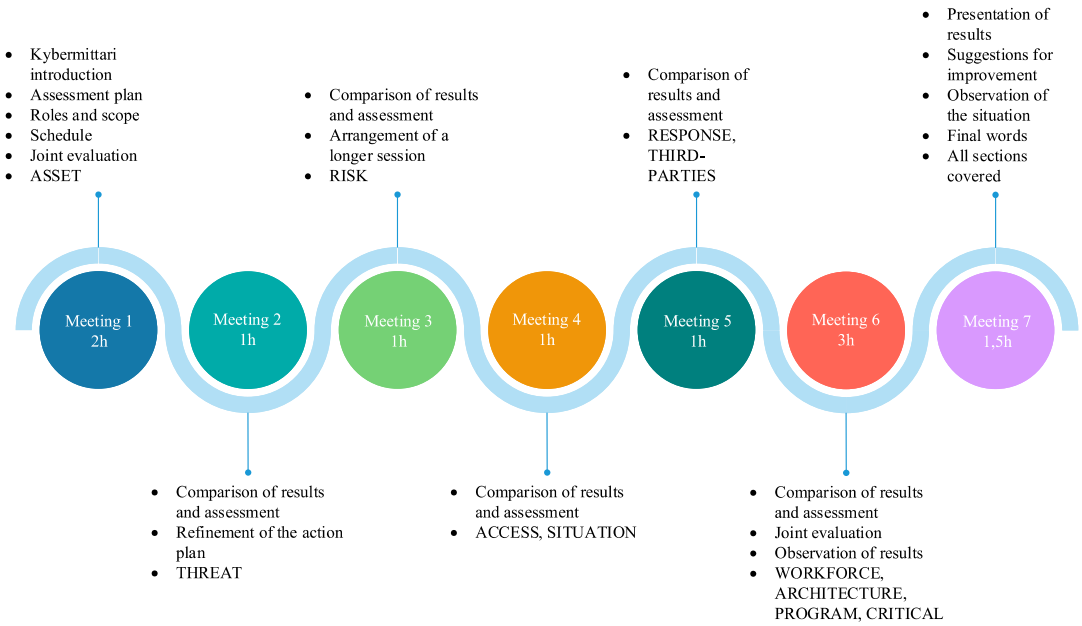

Figure 6.1: Assessment Workflow Overview

6.2.1 Observations and Key Challenges

The general opinion was that the Kybermittari-tool was efficient in achieving its objectives. Developed in Microsoft Excel, its navigation was intuitive, given the previously acquired understanding of Excel. The assessment areas were clearly separated by topic and included a general explanation and overview of the area. Since the master version of the results could be stored and accessed via cloud, version control and safeguarding the integrity of information could be automated. A local copy of the results was stored between each session just in case of complications. Also, the automated reports based on the filled fields were deemed exemplary, as these provided detailed information of the results' relation to different scoring criteria and perspectives, including NIST CSF versions 1.1 and 2.0, C2M2 and a general written report targeted for presenting the results to upper management.

Kybermittari also includes tabs for development monitoring and reflection on previous assessments. The option to import or export results from another evaluation and the option to map results based on other frameworks also enable the use of the tool with parallel frameworks while tracking development. In addition, the high level of customization with individual bookmarking of practices and selection of specific development areas enables versatile utilization of the tool depending on the areas of focus and use case.

From a linguistic perspective, the common obstacles in the use of the tool appeared in the interpretation of the practices. The tool offers English, Finnish, or Swedish language options, with the selection being directly applied. As the sections, objectives, and practices are derived from C2M2, except for the CRITICAL section, the Finnish and Swedish versions are translated from the English version. In certain cases, this required a copy of the English version on the side, as certain nuances were lost in translation. For example, in part 1f of the THREAT-tab, the English version emphasizes periodical cybersecurity vulnerability assessments, while

the Finnish version implies irregular and time-to-time assessments. These small nuances were found to affect the evaluation in several cases, as the distinction between irregular and consistent practices has a major difference when evaluating the level of sophistication of a function.

6.3 Results and Analysis

After the evaluation of the predefined 11 sectors, a concluding meeting was held to present and discuss the results and future directions. From the final report generated by the Kybermittari tool, a general overview of strengths and weaknesses was presented, highlighting the organizations' general abilities to control, recognize, protect, identify, respond, and recover from cybersecurity risks and threats. These were derived by cross-referencing the results to the NIST CSF v2.0 framework and as a written report, this is well-suited for presenting the results to the upper management and legal representatives.

The generated reports included a category-based overview, areas of development, general management measures, and a detailed NIST CSF report intended for analyzing, reporting, and guiding internal development of the assessment results. This information was utilized to present the required steps and implemented practices to achieve the next maturity level.

6.3.1 Findings Overview

Utilizing the previously established summary of the foundational risk management measures derived from the draft recommendation for NIS supervisory authorities and presented in Section 5.2, the findings of the assessment can be inspected from the perspective of risk management and governance, operational and system security, and resilience and continuity.

Risk Management and Governance

For the risk management and governance category, the relevant sections of Kybermittari include RISK, THIRD-PARTIES, WORKFORCE, and PROGRAM. These sections evaluate the organization's ability to identify, assess, and manage cybersecurity risks through its risk management program, emphasizing the management of risks holistically, including those posed by the internal workforce, third-parties, and overall organizational structure and cybersecurity management. The best practices direct towards a comprehensive cybersecurity program that aligns with the organization's mission, objectives, and risk management strategy. With relevant cyber risks and third-party dependencies identified, assessed, and prioritized, risks can be managed in a structured and predefined manner with the necessary resources, personnel, and senior management support and involvement.

As the organization under assessment operates globally, the minimum industry requirements, such as the existence of a cyber risk management strategy and program and the identification of third-party dependencies, are achieved through established practices and guidelines from the business concern and regulation. As a baseline, the level 1 practices emphasize the establishment of foundational measures in an ad hoc manner, including practices such as implementation where cyber risks are assessed and prioritized based on their estimated impact, recognition of important IT and OT third-party dependencies, existence of a cybersecurity program strategy, and promotion of activities concerning cybersecurity awareness raising. These practices were unanimously considered to have been implemented.

But with the focus on local operations and specifically the viewpoint of the personnel in charge of the manufacturing network, certain objectives couldn't be definitively marked as implemented. These mainly concerned the documentation and regularity of operations in the fields of risk categorization, evaluation of protection mechanisms, and utilization of established tools for assessing the cybersecurity

readiness of suppliers. The Level 2 practices emphasize a more structured approach with risks categorized and prioritized in a risk register which is maintained, and similarly risks concerning third-parties being individually evaluated and prioritized in a documented manner. Additionally, the emphasis on proactivity is present on Level 2 with independent assessment of cybersecurity competencies and local management involvement in developing, maintaining and enforcement of cybersecurity policies. At Level 3, the focus shifts towards continuous improvement and refinement of the risk management processes including real-time assessments, regular audits and active cybersecurity policy effectiveness evaluation.

While the foundational measures were deemed as implemented, the responsibilities highlighted at level 3 were perceived as intensive but achievable through cross-departmental collaboration and additional resources. Key focus areas for development include continuous communication with relevant entities, along with the allocation of dedicated personnel and the establishment of clear accountability structures to ensure the effective execution of advanced cybersecurity practices. In addition, a revision of the local cyber risk management strategy and program was added to the action plan.

Operational and System Security

In the operational and system security category, the relevant sections concern the ASSET, THREAT, ACCESS, and ARCHITECTURE sections. With a focus on technical implementations, this category focuses on a risk-based approach to threat mitigation, vulnerability management, and the maintenance of security activities for hardware, software, data, and access rights. The best practices guide the development of a cybersecurity architecture that enables the identification, mitigation, and response to cyber threats in a sufficient capacity through proactive measures, efficient information sharing, and risk-based controls which ensure an acceptable level

of protection and resilience.

Level 1 practices emphasize the foundational and ad hoc establishment of robust security measures, controls, and an architecture that promotes cybersecurity, including basic network and endpoint protections. On Level 2, the requirements become more detailed with risk profiling, prioritization concerning individual assets and data types, and the incorporation of principle of least privilege. On Level 3, the focus shifts to continuous monitoring, maintenance, and analysis of the effectiveness of the implemented measures throughout their lifecycle. This includes purpose-built solutions for end-point detection and response, active log analysis, anomaly detection, identity verification, and the refinement of the cybersecurity architecture.

From a technical standpoint, the implementations were deemed exemplary. Key measures include comprehensive asset inventory management and security configurations, segmentation of critical information repositories, regular vulnerability scanning, structured backup procedures, and strong physical and logical access control measures, reinforced by multi-factor authentication. To achieve a higher maturity level, more detailed practices are required, including comprehensive asset inventory management with prioritized classifications based on operational significance, ongoing maintenance of the risk profile registry, enhanced protection of stored data for specific data types, and additional safeguards to prevent data destruction.

This shift expresses the need for a more structured and precise approach towards cybersecurity risk management, ensuring that critical assets and sensitive data are identified and appropriately protected. To keep the process sustainable, the processes require regular assessment to maintain alignment with evolving threats and business priorities.

Resilience and Continuity

In the context of resilience and continuity, the relevant sectors of Kybermittari include SITUATION, RESPONSE and CRITICAL. Situational awareness and effective incident response are central to the continuity of operations. The organization's ability to maintain an understanding of their cybersecurity environment and anticipate potential threats allows the utilization of processes and controls to detect, analyze and recover from incidents, ensuring operational and business continuity. Identifying critical services further ensures that societal and organizational stability can be maintained, minimizing the impact of disruptions and supporting long-term resilience.

At Level 1, the practices focus on foundational measures, including the collection and review of logs from assets essential for operations, as well as establishing communication channels for reporting anomalies and cybersecurity events and strategy and relevant tools to restore operations in the event of a cybersecurity incident, with designated incident response personnel identified. For critical services, the practices include identification and documentation of these services, along with a response plan covering them and inclusion within risk management policies. Level 2 introduces more advanced practices such as prioritized log analysis, aggregation of log data, and refinement of incident and response plans, while establishing accountability at the board level of operations. At Level 3, incident response is integrated with business strategies, enhancing monitoring for high-priority assets and refining response and continuity plans based on ongoing risk assessments and testing in a proactive manner.

During the assessment, it was concluded that the requirements of logging activities primarily focus on their existence. In other words, while logging requirements are present, further definition and maintenance would be beneficial. While important IT and OT equipment receive the appropriate attention, the evaluation of other

operations proved to be difficult due to the lack of certainty and knowledge regarding the areas.

As a result, log collection and analysis were identified as areas for potential development. The criteria for assessing the impact of potential incidents on specific functions could benefit from further refinement, along with continuity plans, particularly in terms of asset replacement and definitions of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). The critical section faced some challenges, as the assessment did not fully focus on activities that are vital to society. However, from a production network perspective, it was observed that overall policies address the key requirements. This section could also be improved with more detailed information from relevant personnel.

6.3.2 NIS2 and HE 57/2024

The Government Proposal HE 57/2024 outlines Finland's legislative adaptation for implementing the NIS2 Directive [28] and serves as a key reference for assessing an organization's NIS2 readiness. This section analyzes the Kybermittari results in the context of NIS2 requirements and its Finnish implementation and contextualizes the results within them. Appendix A illustrates the mapping of Kybermittari sections to the subchapters of Article 9 of HE 57/2024, which outlines the key measures to manage cybersecurity risks. Following a similar division as before, the subchapters of the legislation will be analyzed through the perspectives of risk management and governance, operational and system security, and resilience and continuity.

Risk Management and Governance

As discussed in Chapter 3 and Section 3.2.1, NIS2 mandates a comprehensive, risk-based approach to cybersecurity. While each sub-area of organizational cybersecurity addresses administrative measures to a certain degree, the primary risk man-

agement and governance measures under Article 9 in HE 57/2024 are introduced in subchapters 1 and 6.

Subchapter 1 emphasizes the need for regular maintenance and assessment of a cybersecurity risk management operation policy. This requires documented proof that the organization is capable of recognizing, evaluating, and managing risks. With the emphasis on regularity, the policies must include regular reviews to ensure measures remain effective and aligned with strategic objectives. Risks should be prioritized for mitigation, elimination, or externalization with regular assessments, conducted internally or by a third party using appropriate metrics.

Subchapter 6 focuses on managing personnel-related security risks. It outlines responsibilities, necessary skills, background checks, work rotation risks, and cybersecurity training to ensure employees are aware and capable of fulfilling their roles securely and efficiently.

As acknowledged in Section 6.3.1, the Kybermittari assessment revealed that while foundational risk management and governance practices are in place, documentation and systemic evaluation, specifically concerning risk categorization and policies regarding third parties may require further formalization to meet the regulatory expectations outlined in HE 57/2024. Although it has been highlighted that the measures should be proportionate to the organization's size, risk exposure, and sector-specific requirements, the emphasis remains on maintaining a structured and proactive cybersecurity posture.

Operational and System Security

From an operational and system security standpoint, the relevant sections in Article 9 of HE 57/2024 include subchapters 2, 3, 5, 7, 8, 9, and 11. Subchapters 2 and 3 cover network and information systems security from the perspective of acquisition, development, and maintenance. With subchapters 5, 7, 8, 9, and 10, the focus shifts

towards the management of critical assets, procedures and policies for authentication and encryption, deviation analysis, and basic cybersecurity practices. With the focus on aligning organizational operations to cover the entire lifecycle of assets and services, the security measures must be up-to-date, prioritized based on asset criticality, and ensure adequate protection in terms of confidentiality, authenticity, and integrity.

On a practical level, this involves maintaining a comprehensive asset inventory, implementing and regularly updating security configurations that align with the organizational cyber security requirements, and managing vulnerabilities based on risk. While ISO 27001 provides a strong foundation for the requirements of cybersecurity policies, the measures should be implemented to fit the specific needs of the organization. In addition to securing assets, attention should be given to access control, authentication, and monitoring, with proper staff training and background checks.

As reflected on Section 6.3.1, the relevant procedures and policies regarding operational and system security were the strongest sections in the assessment and can be deemed sufficient to meet the criteria established in HE 57/2024. Through the organization's compliance with the GxP-framework (Good x Practice) set by the Medicines & Healthcare Products Regulatory Agency (MHRA), practices and policies regarding data integrity and operational security must be strong and exemplary. The requirements mandate risk-based controls to ensure the completeness, consistency, accuracy, and security of data throughout its lifecycle. Additionally, obliged and implemented measures like audit trails, metadata management, secure access controls, encryption, backup management, and system validation efficiently prevent unauthorized changes and protect critical assets, while ensuring that any deviations are efficiently detected and addressed. [61]

These practices not only support the core principles of operational and system

security, but also align with the regulatory expectations outlined by HE 57/2024 for maintaining data integrity and confidentiality within the organization. In conclusion, while the measures taken to ensure operational and system security can be considered exemplary, a review of vulnerability prioritization and the implementation of a clear classification can provide a more holistic foundation for operational and system security. As highlighted in NIS2, these operations must be continuous, maintained, and actively considered.

Resilience and Continuity

For resilience and continuity, the relevant sections of Article 9 of HE 57/2024 include subchapters 4, 10 and 12. These cover supply chain security, business continuity, and physical security. As depicted in Figure A.2, a list of suppliers and service providers is expected from the entities under regulation. In addition, the effects of disruption and internal and external supply chain vulnerabilities should be noted in the risk management measures. Backup and recovery policies should also be in place to assure that the entity is able to continue its operations in the case of disruptions or incidents.

These measures involve proper backup management and security; in other words, assuring that all critical systems and data have an appropriate backup frequency, level of protection, and are tested to assure that operations can be efficiently restored. For third-parties, regular risk assessments could be conducted and with the implementation of clear Service-Level Agreements (SLA), the cyber requirements expected of them can be contractually agreed upon. While the CER Directive applies to the majority of NIS2 critical entities and covers physical security measures and procedures for incident recovery, measures such as access controls, surveillance, secure storage, and visitor management are expected from all NIS2 entities. These measures are intended to ensure robust cybersecurity risk management.

Similarly, GxP compliance also emphasizes resilience and continuity, with policies addressing backup and recovery processes and ensuring that data ownership, governance, and accessibility are included in contracts with third parties. While the backup, recovery, and physical security procedures were found to be strong during the evaluation, the indirect link between the manufacturing network's impact on critical infrastructure and societal importance resulted in difficulties in evaluating the practices. This revealed that there is a need for greater clarity in assessing the potential impact of incidents on specific business functions as these also concern the manufacturing network. This refinement would help in prioritizing recovery efforts and aligning them with the organization's critical operations.

6.3.3 Next Steps for Improvement and Reproducibility

Early on, it was noted that the lack of regularly maintained documentation and prioritization of practices, at least in a summarized and presentable way, was penalizing several sections of the assessment. During the evaluation, discussions regarding certain sections were primarily resolved by considering the question: If an assessor were to request written evidence for this, what documentation could be provided? Since this was the first time utilizing Kybermittari, it was expected that not all necessary information could be gathered due to time constraints. In future assessments, allocating more time to clarify uncertain sections would be beneficial.

As the team was comprised from only personnel within the unit, it was also noted that certain segments couldn't be evaluated due to the lack of certainty. To improve assessment accuracy, it would be beneficial to include personnel from other departments, such as business and management to support the assessment in an advisory role. Since maturity assessments are a recurring process, it is also expected that the results and key areas of improvement are considered and utilized in the next assessment. While the frequency of assessments should be adjusted to support

changes in environment, and be proportionate to the entities risks and maturity level, it is generally recommended that organizations conduct assessments at least annually to ensure ongoing compliance, identify emerging vulnerabilities, and track improvements. This frequency allows organizations to stay aligned with evolving threats, regulatory requirements, and internal changes. [62] By taking the recognized and documented areas of improvement into consideration and implementation, the next assessment should include the results from the previous evaluation, and this is supported by the import-tab in Kybermittari.

A total of 11 hours was spent together introducing the subject matter, the Kybermittari-tool, the timetable, as well as the evaluation, presentation of results, and reflection. During this period, the current state of cybersecurity of the manufacturing network was evaluated based on the 11 assessment areas of Kybermittari and the maturity levels of these domains was obtained. Based on the results, a recommendation guide was comprised and presented. With a clear understanding of key areas of improvement, the next steps involve addressing the identified gaps, with an emphasis on refining the documentation processes, as also improving cross-functional and managerial involvement. Overall, the assessment results provide a strong baseline for ongoing cybersecurity improvements and serve as a reference for ensuring that the manufacturing network remains secure and resilient in the face of emerging threats.

7 Conclusions

This thesis has examined the current state of cybersecurity by analyzing the cybersecurity landscape from global, national, and critical infrastructure perspectives, the requirements imposed by the NIS2 Directive and the role of cybersecurity maturity models in identifying regulatory gaps. With the enforcement of the NIS2 Directive, organizations across Europe face stricter security requirements to mitigate emerging threats, requiring an ongoing process of self-assessment, which this study aims to support and expand upon.

7.1 Practical Applications

Although the assessment presented was centered around the operations of the manufacturing network, the approaches and methodologies used in this study are generally applicable by entities subject to NIS2 or any organization aiming to enhance their cybersecurity and risk management posture. As the NIS2 Directive promotes proportionality of measures and sector-specific focus areas, the general results of assessments must be interpreted contextually, with the focus on identifying crucial functions, their weaknesses, and strategies to address shortcomings while promoting continuous development.

The findings of this study provide a basis for organizations on how to independently conduct a cybersecurity maturity assessment in a fixed time-frame and with a predefined amount of personnel. With a thorough explanation of the NIS2 Directive

and its implementation in Finland, including its reasoning, content, requirements, and implications, this study helps organizations to understand the responsibilities invoked by NIS2 and to align their practices to achieve compliance.

7.2 Summary of Findings and Final Words

The introduction of this thesis presented two research questions that formed the foundation of the study. The first research question (*How can cybersecurity maturity models be used to evaluate and improve organizations' information security and compliance with the NIS2 directive?*) is addressed through a review of the NIS2 directive and existing cybersecurity frameworks, an analysis of their capacity to provide insights into information security, and a systematic cybersecurity assessment. After introducing the requirements set by NIS2, various evaluation tools and frameworks were analyzed, and Kybermittari was selected as the suitable tool for conducting the assessment. The findings of the assessment indicate that while the framework aligns well with regulatory expectations concerning risk management, security, and resilience improving measures, maturity evaluation can improve an organization's information security only when areas for improvement are acknowledged and a structured plan for achieving a higher maturity level is followed.

The second research question (*What are the strengths, weaknesses, and applicability of cybersecurity maturity models in the context of NIS2 requirements?*) revolves around evaluating the tool used in the assessment and the results obtained. The analysis considered both the strengths and limitations of the tool, particularly its ability to support organizations in identifying necessary security measures. The key findings of the assessment indicate that while the technical measures and cohesive approach to cybersecurity align well with regulatory expectations, prioritization, incident response readiness and continuous monitoring could be considered as areas for further development. These weaknesses were recognized through the Kybermittari

tool, highlighting its strength in identifying critical areas for improvement. Additionally, it was acknowledged that maturity evaluation requires extensive knowledge of the operations of the organizations and this should be noted in the selection of evaluators. This process is most effective when conducted periodically and is able to improve organizations information security only if areas for improvement are acknowledged.

Cybersecurity maturity models are effective in mapping and identifying an organization's cybersecurity capabilities holistically, while promoting continuous improvement, as required by NIS2. However, their effectiveness depends on an in-depth understanding of the organization's operations and demands time, expertise, and commitment from senior management. In terms of applicability, these models are highly relevant for NIS2 compliance. Specifically, Kybermittari is highly customizable to an organization's context, as NIS2 emphasizes proportionality in actions and provides actionable insights that can help develop targeted improvement plans. In the context of NIS2 auditing, the results of the assessment can also be used to support proof of evaluation and aid in providing documentation when needed.

In conclusion, this thesis has explored the use of cybersecurity maturity models, specifically Kybermittari, in evaluating and improving organization's compliance with the NIS2 Directive. It also expanded on the understanding of NIS2, detailing its requirements and the impact it has across Europe, while providing a clear and accessible outline of its key sections. The study's practical implications are relevant for organizations seeking to meet the NIS2 requirements and offers valuable insights into the measures expected of them and the applicability of maturity models in real-world scenarios. The study's limitations, such as the scope of the assessment and focus on a single tool, suggests opportunities for further research by expanding this work on monitoring the development of cybersecurity maturity overtime and further addressing the complications of NIS2. Ultimately, this thesis contributes to the

ongoing development and awareness of cybersecurity and supports organizations in navigating the complexities of NIS2 and other relevant and forthcoming legislation.

References

[1] International Business Machines Corporation, *Cost of a data breach 2024*. [Online]. Available: https://www.ibm.com/reports/data-breach (visited on 11/28/2024).

[2] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2023*, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[3] European Union Agency for Cybersecurity, *ENISA Threat Landscape 2024*, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[4] European Union, *NIS2 Directive: new rules on cybersecurity of network and information systems*. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (visited on 11/27/2024).

[5] N. Vandezande, "Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor", *Computer Law & Security Review*, vol. 52, 2024. DOI: 10.1016/j.clsr.2023.105890.

[6] S. Valavanis, "Understanding Cybersecurity Maturity in Practice", *Journal of Information Systems*, vol. 38 (3), pp. 1–5, 2024. DOI: 10.2308/ISYS-2024-026.

[7] World Economic Forum, *Global Risks Report 2024, 19th edition*, 2024. [Online]. Available: https://www.weforum.org/publications/global-risks-report-2024/digest/.

[8] D. Weston, *Helping our customers through the CrowdStrike outage*, The Official Microsoft Blog. [Online]. Available: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/ (visited on 11/28/2024).

[9] International Telecommunication Union, *Global Cybersecurity Index*. [Online]. Available: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (visited on 11/28/2024).

[10] National Cybersecurity Security Index, *NCSI: Finland, archived data from 2016-2023*. [Online]. Available: https://ncsi.ega.ee/country/fi_2022/ (visited on 12/02/2024).

[11] Yleisradio Oy, *Pro-Russia hacker group suspected of targeting Finnish parliament, Sanna Marin websites with DoS attack*. [Online]. Available: https://yle.fi/a/74-20025824 (visited on 12/02/2024).

[12] National Cyber Security Centre Finland, *Information security in 2023*, 2024. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/en/publications/information-security-2023.

[13] Australian Cyber Security Centre, *Identifying and Mitigating Living Off the Land Techniques*. [Online]. Available: https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/identifying-and-mitigating-living-off-the-land-techniques (visited on 12/02/2024).

[14] A. Perdana *et al.*, *FraudGPT and other malicious AIs are the new frontier of online threats. What can we do?* [Online]. Available: http://theconversation.

com/fraudgpt-and-other-malicious-ais-are-the-new-frontier-of-online-threats-what-can-we-do-234820 (visited on 11/28/2024).

[15] German Institute for International and Security Affairs, *European Repository of Cyber Incidents (EuRepoC)*. [Online]. Available: https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc (visited on 12/02/2024).

[16] Cybersecurity and Infrastructure Security Agency, *APT Cyber Tools Targeting ICS/SCADA Devices | CISA*, 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a (visited on 12/02/2024).

[17] Dragos Inc., *CHERNOVITE Threat Activity Group*. [Online]. Available: https://www.dragos.com/threat/chernovite/ (visited on 12/02/2024).

[18] International Business Machines Corporation, *IBM Security X-Force Threat Intelligence Index 2024*. [Online]. Available: https://www.ibm.com/reports/threat-intelligence (visited on 12/06/2024).

[19] European Union, *Directive (EU) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union*, Official Journal of the European Union, L 194/1, 2016. [Online]. Available: http://data.europa.eu/eli/dir/2016/1148/oj.

[20] NIS Cooperation Group, *Reference document on Incident Notification for Operators of Essential Services. Circumstances of notification*, CG Publication 02/2018, 2018. [Online]. Available: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf.

[21] A. Monica *et al.*, "Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)", *Publications Office of the European Union*, 2021. DOI: 10.2759/184749.

[22] European Union, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union*, Official Journal of the European Union L333/80, 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj.

[23] European Union, *Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024*, Official Journal of the European Union L series, 2024. [Online]. Available: http://data.europa.eu/eli/reg_impl/2024/2690/oj.

[24] European Union Agency for Cybersecurity, *Asking for your feedback: ENISA technical guidance for the cybersecurity measures of the NIS2 Implementing Act*. [Online]. Available: https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act (visited on 01/14/2025).

[25] European Union, *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises*, Official Journal of the European Union L124, 2003. [Online]. Available: http://data.europa.eu/eli/reco/2003/361/oj/eng.

[26] National Cyber Security Centre, *NCSC: NIS2 Essential and Important Entities*, 2023. [Online]. Available: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_2_ENTITIES.pdf.

[27] Finnish Transport and Communications Agency Traficom, *LUONNOS suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimen-*

piteistä, Traficom/18410/09.00.02/2023, 2024. [Online]. Available: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=ebc51269-712e-4115-b137-b0b2a710dac4.

[28] Finnish Parliament, *Hallituksen esitys HE 57/2024 vp*, 2024. [Online]. Available: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_57+2024.aspx.

[29] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, 2022.

[30] The White House, *National Security Presidential Directive (NSPD-54) / Homeland Security Presidential Directive (HSPD-23)*, 2008. [Online]. Available: https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[31] Committee on National Security Systems, *CNSSI 4009: Committee on National Security Systems Instruction*, 2022. [Online]. Available: https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

[32] T. Mettler, "Maturity assessment models: A design science research approach", vol. 1/2, pp. 81–98, 2011. DOI: 10.1504/IJSSS.2011.038934. (visited on 01/13/2025).

[33] J. M. Song *et al.*, "Does cybersecurity maturity level assurance improve cybersecurity risk management in supply chains?", *International Journal of Accounting Information Systems*, vol. 54, DOI: https://doi.org/10.1016/j.accinf.2024.100695. (visited on 01/13/2025).

[34] European Commission, Directorate-General for Communications Networks, Content and Technology, *ISO/IEC 27001 - The international standard for information security.* [Online]. Available: https://digital-skills-jobs.

europa.eu/en/inspiration/resources/isoiec-27001-international-standard-information-security (visited on 12/11/2024).

[35] A. P. Aldya *et al.*, "Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard", *IOP conference series. Materials Science and Engineering*, vol. 550, no. 1, 2019, ISSN: 1757-8981. DOI: 10.1088/1757-899X/550/1/012020.

[36] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27004:2016 – Information Technology — Security Techniques — Information Security Management — Monitoring, Measurement, Analysis and Evaluation*, 2016.

[37] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, 2024. DOI: 10.6028/NIST.CSWP.29.

[38] Certified Information Security, *A Certified NIST Cybersecurity Framework 2.0 Lead Implementer (CSF LI)*. [Online]. Available: https://niccs.cisa.gov/education-training/catalog/certified-information-security/certified-nist-cybersecurity-framework-20 (visited on 02/21/2025).

[39] U.S. Department of Energy, *Cybersecurity Capability Maturity Model (C2M2)*. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (visited on 11/07/2024).

[40] U.S. Department of Energy, *About the Cybersecurity Capability Maturity Model (C2M2)*. [Online]. Available: https://c2m2.doe.gov/about (visited on 11/07/2024).

[41] National Institute of Standards and Technology, *Cybersecurity Capability Maturity Model to NIST Cybersecurity Framework Mapping*. [Online]. Available: https://www.nccoe.nist.gov/news-insights/cybersecurity-capability-

maturity-model-nist-cybersecurity-framework-mapping (visited on 02/21/2025).

[42] International Organization for Standardization, *ISO 13485:2016 - Medical Devices - Quality Management Systems - Requirements for Regulatory Purposes*, 2016.

[43] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 17025:2017 - Testing and calibration laboratories*, 2017.

[44] J. Boehm *et al.*, *The approach to risk-based cybersecurity*, McKinsey & Company. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-risk-based-approach-to-cybersecurity (visited on 11/13/2024).

[45] E. Bonnie, *7 Benefits of Continuous Monitoring & How Automation Can Maximize Impact*, Secureframe. [Online]. Available: https://secureframe.com/blog/continuous-monitoring-cybersecurity (visited on 11/13/2024).

[46] European Union, *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*, Official Journal of the European Union L 333/1, 2022. [Online]. Available: http://data.europa.eu/eli/reg/2022/2554/oj.

[47] European Union Agency for Cybersecurity, *Cybersecurity Policies*. [Online]. Available: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies (visited on 11/05/2024).

[48] European Union Agency for Cybersecurity, *National Cybersecurity Assessment Framework (NCAF) Tool*. [Online]. Available: https://tools.enisa.

europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cybersecurity-assessment-framework-ncaf-tool#/ (visited on 11/07/2024).

[49] European Union Agency for Cybersecurity, *CSIRT Maturity Framework*. [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity (visited on 11/07/2024).

[50] European Union Agency for Cybersecurity, *Cybersecurity Maturity Assessment for Small and Medium Enterprises*. [Online]. Available: https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises (visited on 11/07/2024).

[51] National Cyber Security Centre Finland, *Kybermittari - Cybermeter*. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter (visited on 11/07/2024).

[52] Information Management Board of Finland, "Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) : Suositus ja kriteeristö", *Valtiovarainministeriö*, 2022. [Online]. Available: http://urn.fi/URN:ISBN:978-952-367-275-8.

[53] Center for Internet Security, *CIS Critical Security Controls*, version 8.1, 2024. [Online]. Available: https://www.cisecurity.org/controls/.

[54] Cybersecurity and Infrastructure Security Agency, *Zero Trust Maturity Model*, version 2.0, 2023. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model.

[55] Information Systems Audit and Control Association, *COBIT - Control Objectives for Information Technologies*. [Online]. Available: https://www.isaca.org/resources/cobit (visited on 11/07/2024).

[56] Microsoft Corporation, *Announcing the Microsoft Sentinel: Cybersecurity Maturity Model Certification (CMMC) 2.0 Solution*, Microsoft Sentinel Blog. [Online]. Available: https://techcommunity.microsoft.com/blog/microsoftsentinelblo announcing-the-microsoft-sentinel-cybersecurity-maturity-model-certification-cmm/3295095 (visited on 11/13/2024).

[57] B. Axel *et al.*, *Using the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*. IBM Redbooks, 2013, ISBN: 9780738437897.

[58] National Cyber Security Centre Finland, *Kybermittari-aineistot - Import-työkalu (3.2.2025)*. [Online]. Available: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari/kybermittari-aineistot (visited on 02/11/2025).

[59] National Institute of Standards and Technology, "About NIST", [Online]. Available: https://www.nist.gov/about-nist (visited on 11/14/2024).

[60] A. Calder, *ISO 27001/ISO 27002 - A Guide to Information Security Management Systems*, 1st ed. IT Governance Publishing, 2023, ISBN: 1787784940.

[61] Medicines and Healthcare products Regulatory Agency, *Guidance on GxP data integrity*. [Online]. Available: https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity (visited on 02/20/2025).

[62] K. Dempsey *et al.*, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations", no. NIST Special Publication (SP) 800-137, 2011. DOI: 10.6028/NIST.SP.800-137.

Appendix A Kybermittari Mapping to HE57/2024

Figure A.1: Kybermittari mapping to subchapters of HE57/2024. Chapters 1 and 2. Adapted from [27], [58]

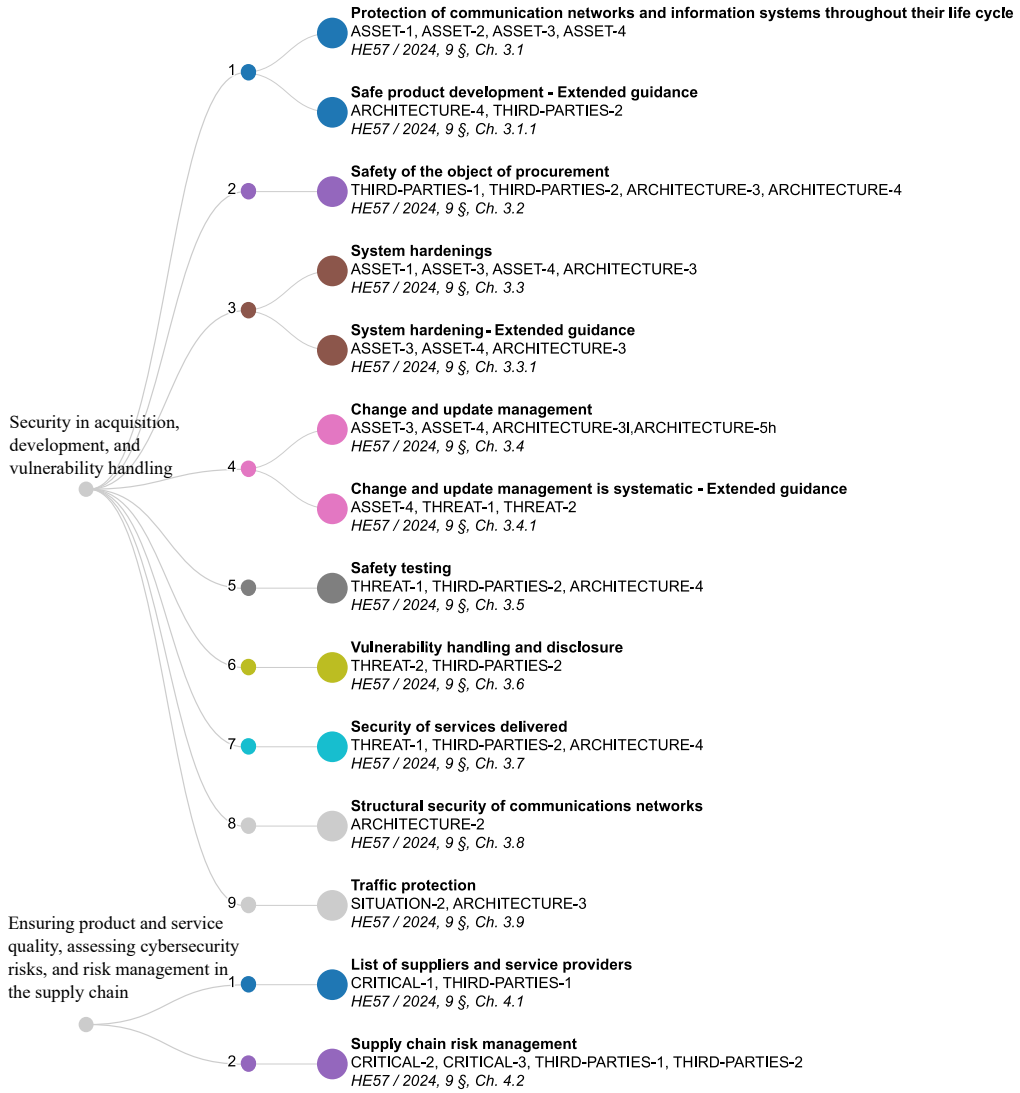

Figure A.2: Kybermittari mapping to subchapters of HE57/2024. Chapters 3 and 4. Adapted from [27], [58]

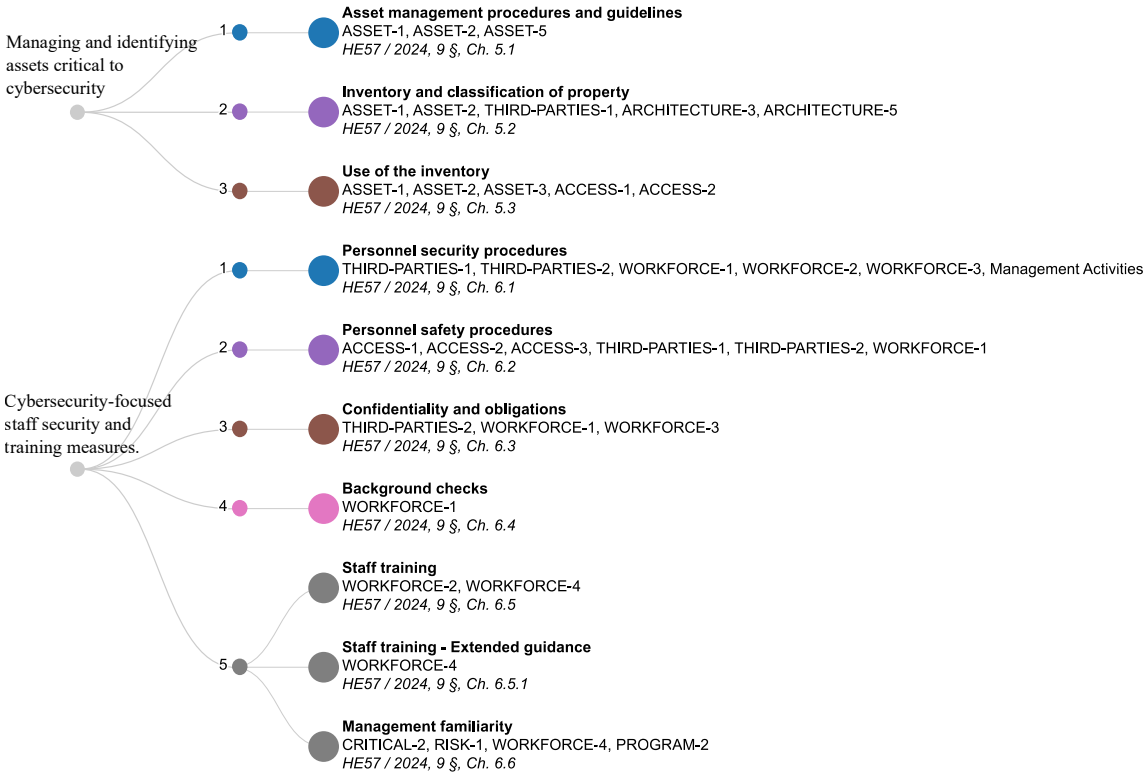

Figure A.3: Kybermittari mapping to subchapters of HE57/2024. Chapters 5 and 6. Adapted from [58]

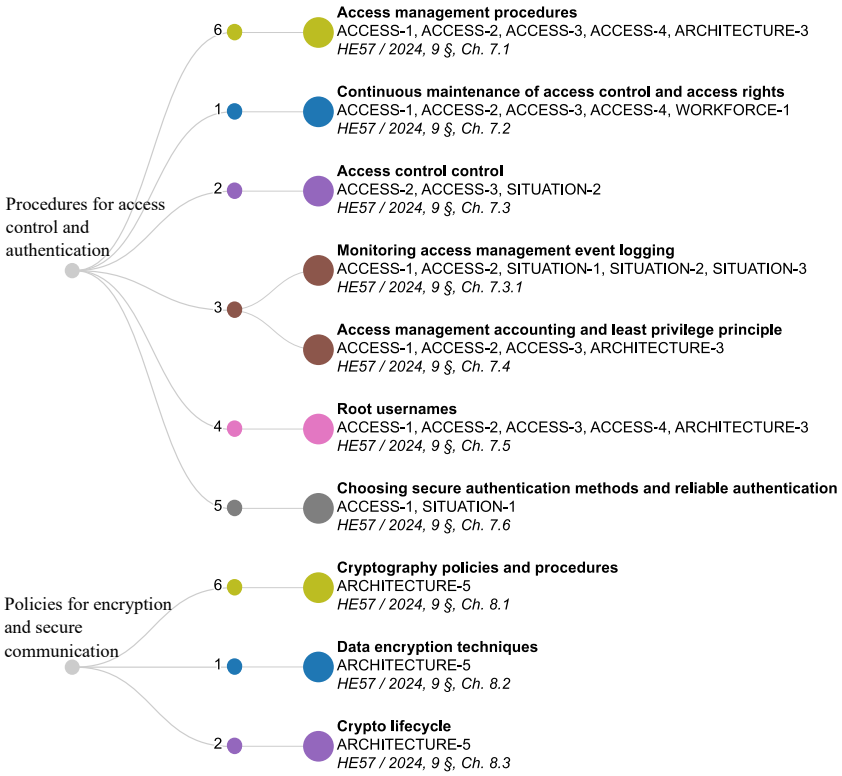

Figure A.4: Kybermittari mapping to subchapters of HE57/2024. Chapters 7 and 8. Adapted from [27], [58]

Figure A.5: Kybermittari mapping to subchapters of HE57/2024. Chapters 9 and 10. Adapted from [27], [58]

Figure A.6: Kybermittari mapping to subchapters of HE57/2024. Chapters 11 and 12. Adapted from [27], [58]