A comprehensive analysis of the NIS2 implementation in international companies in Finland through the ISO/IEC 27001 framework

University of Turku
Department of Computing
Master of Science Thesis
Cyber Security Engineering
July 2026
Abrar, Ehsanul

Supervisors:
Antti Hakkala
Tahir Mohammad

UNIVERSITY OF TURKU
Department of Computing

ABRAR, EHSANUL: A comprehensive analysis of the NIS2 implementation in international companies in Finland through the ISO/IEC 27001 framework

Master of Science Thesis, 61 p.
Cyber Security Engineering
July 2026

This MSc thesis investigates how international companies operating in Finland can implement the EU's NIS2 Directive using the ISO/IEC 27001:2022 framework as their primary compliance instrument. Through a systematic, control-by-control mapping between NIS2 provisions-particularly risk management (Article 21), incident reporting (Article 23), and supply chain security (Article 21(2)(d))-and the 93 controls of ISO 27001, the study identifies direct alignments, partial overlaps, and complete gaps. The analysis reveals that approximately 63.6% of NIS2's risk management requirements are fully addressed by existing ISO controls, while critical gaps remain in binding incident reporting timelines (24-hour, 72-hour, and one-month deadlines), multi-factor authentication prescriptiveness, individual supplier vulnerability assessment granularity, and management liability. To address these gaps, the thesis proposes six supplementary measures (S1-S6), including a dedicated NIS2 incident reporting procedure, mandatory MFA policy, per-supplier vulnerability assessment templates, and formalised management accountability. The outcome is an evidence-based, phased implementation model that enables organisations to extend their existing Information Security Management Systems (ISMS) for full NIS2 compliance without requiring re-certification. The findings provide actionable insights for practitioners navigating the evolving regulatory landscape in Finland, particularly in light of the national implementation proposal HE 57/2024, and contribute to the broader academic discourse on standard-regulation alignment in cybersecurity governance.

Keywords: NIS2 Directive, ISO/IEC 27001, information security management systems (ISMS), cybersecurity regulation, compliance implementation, information security, risk management

Acknowledgements

This thesis was written independently by the author based on the understanding and learning outcomes acquired throughout the Master's programme in Cyber Security at the University of Turku. The research was conducted during the author's studies at the Department of Computing, Faculty of Technology, with valuable guidance and supervision provided by the thesis supervisors. I would like to express my sincere gratitude to my supervisors for their insightful feedback, continuous support, and constructive guidance throughout the research process. Their expertise and encouragement were instrumental in shaping this thesis and ensuring its academic rigour. I am also grateful to the University of Turku for providing the academic environment and resources necessary to complete this research. The support from the Department of Computing, particularly the Cyber Security programme, has been invaluable in developing the knowledge and skills required for this study. Various scientific research articles, official EU legal documents, ISO standards, and technical reports were used as references and are cited accordingly in the Reference section. These sources provided the foundational knowledge and empirical basis for the analysis presented in this thesis. In addition, some free and basic online LLM/AI tools were utilised solely for structurisation and paraphrasing purposes. The DeepSeek and Gemini LLMs were employed to facilitate the organisation and structuring of the thesis content, particularly in summarising and refining complex regulatory texts to improve clarity and coherence. The mybib IEEE Citation Generator was used to

create the required citations for research articles and official documents, ensuring accurate and consistent IEEE formatting throughout the thesis. All core analysis, mapping decisions, interpretations, and conclusions presented in this thesis are the author's own work. The use of AI tools was limited to assisting with structure and reference management, and did not replace the author's independent research, critical thinking, or original contribution to the field. Finally, I thank my family, friends, and colleagues for their understanding, encouragement, and patience during this demanding academic journey. Their unwavering support has been a constant source of motivation.

Contents

List of Figures

List of Tables

1 Introduction

In the contemporary digital epoch, the complexity and prevalence of cyberattacks present substantial hurdles for organizations globally. Empirical data reveal a significant escalation in both the occurrence and economic ramifications of cyber incidents impacting organizations. For instance, as reported in IBM's Cost of a Data Breach Report 2025, the global average expenditure associated with a data breach in 2025 is projected to be USD 4.44 million, reflecting a 9% reduction from the preceding year, while simultaneously indicating a 15% augmentation over the last three years, with incidents involving multiple environments incurring an average cost of USD 5.05 million [1]. This, coupled with the 4,875 incidents documented within the EU from July 2024 to June 2025, underscores the imperative for more stringent cybersecurity policies within the European Union [2].

Acknowledging the necessity for robust and uniform cybersecurity protocols across member states, the European Union has initiated measures to confront the dynamic landscape of cybercrime through the revised Network and Information Security Directive (NIS2), broadening its applicability to additional sectors [3]. By accentuating augmented measures for risk management, reporting responsibilities, and resilience, NIS2 renders critical industries, along with their senior management, accountable for their cybersecurity practices. While the NIS2 Directive compels organizations to implement specific strategies to guarantee resilience against cyber threats, it refrains from directly stipulating a particular implementation framework

or supplying detailed methodologies for assessing and attaining the requisite level of compliance [3]. The transposition deadline of 17 October 2024 has elapsed, and on 7 May 2025, the European Commission issued a reasoned opinion to 19 Member States-including Finland-for their failure to notify full transposition of the NIS2 Directive [4].

Organizations may encounter challenges in executing the stipulations delineated in the directive owing to a deficiency in comprehension regarding the efficacy and scope of their pre-existing cybersecurity measures. Through individualized interpretation and implementation of the requirements predicated on the unique contexts of organizations, discrepancies may manifest concerning the compliance approaches adopted by various entities. Given that disproportionate and inadequate implementations, ambiguous definitions, and insufficient cooperation among member states have been identified as significant deficiencies of the original Network and Information Security Directive [5], the necessity for standardized, internationally recognized frameworks to guide organizations toward compliance becomes increasingly apparent.

The ISO/IEC 27001:2022 framework offers a methodical, risk-centric approach for organizations to establish, execute, sustain, and perpetually enhance an Information Security Management System (ISMS) [6]. With its extensive array of 93 controls reorganized into four thematic categories (organizational, people, physical, and technological), ISO 27001 furnishes a globally acknowledged baseline for information security management that numerous international corporations have already adopted. An appropriate alignment between the requirements of NIS2 and the controls of ISO 27001 can serve as a powerful instrument to address regulatory deficiencies and delineate essential measures for compliance. This thesis aspires to bridge the divide between the stipulations of the NIS2 Directive and the ISO 27001 framework by examining their alignment, identifying gaps and synergies, and formu-

lating an integrated implementation model for international enterprises operating in Finland.

1.1 Background and Problem Statement

The increasing frequency and financial impact of cyberattacks-the global average cost of a data breach reached USD 4.44 million in 2025, with 4,875 incidents observed in the EU-have driven the EU to adopt the NIS2 Directive [1]–[3]. NIS2 mandates stricter risk management, incident reporting (early warning within 24 hours), supply chain security, and management accountability, but it does not prescribe a specific implementation framework [3]. International companies in Finland must also navigate the national implementation proposal (HE 57/2024) and other regulations such as GDPR and DORA [7], [8]. This flexibility creates uncertainty: organisations lack a structured, auditable pathway to demonstrate compliance. The ISO/IEC 27001:2022 framework, with its 93 controls and certifiable ISMS, offers a globally recognised foundation that many international firms already use [6]. However, a systematic, control-by-control mapping between NIS2 requirements (as transposed into Finnish law) and ISO 27001 controls-including an analysis of gaps and supplementary measures-is missing.

1.2 Research Objectives and Questions

The primary objective of this thesis is to provide a systematic analysis of how international companies operating in Finland can leverage the ISO/IEC 27001 framework to achieve compliance with the NIS2 Directive. To achieve this, the study pursues the following specific objectives:

- **RO1:** To map the cybersecurity requirements of the NIS2 Directive - as implemented in Finland through HE 57/2024 - onto the controls of ISO/IEC

27001:2022, identifying direct alignments, partial overlaps, and complete gaps.

- **RO2:** To evaluate the strengths and limitations of using ISO 27001 as a primary compliance tool for NIS2, with particular focus on three critical provisions: risk management, incident reporting, and supply chain security.
- **RO3:** To identify supplementary measures required where ISO 27001 controls fall short of NIS2 obligations, and to propose an integrated implementation model for international companies in Finland.

Based on these objectives, the thesis addresses the following research questions:

1. **RQ1:** How can the ISO/IEC 27001 framework be systematically mapped and utilized to achieve comprehensive compliance with the NIS2 Directive's cybersecurity requirements?
2. **RQ2:** What are the strengths, limitations, and identified gaps when employing ISO 27001 controls to address NIS2 provisions on risk management, incident reporting, and supply chain security?

1.3 Scope and Delimitations

The scope of this thesis is limited to the analysis of how the ISO/IEC 27001:2022 framework can be used to implement the NIS2 Directive (EU 2022/2555) in the context of international companies operating in Finland. The study focuses exclusively on the twelve cybersecurity risk management measure categories outlined in the Finnish government proposal HE 57/2024, which transposes NIS2 into national legislation [7]. The analysis is conducted through systematic document analysis and control mapping, without empirical data collection such as interviews or surveys.

Several delimitations apply. First, the thesis considers only the ISO/IEC 27001:2022 standard as the primary compliance framework; other frame-

works (e.g., NIST CSF, C2M2, Kybermittari) are referenced for context but not systematically mapped [6], [9]. Second, the study focuses on three specific NIS2 provisions - risk management (Article 21), incident reporting (Article 23), and supply chain security - as these represent the most challenging areas for organisations [3]. Other provisions, such as those concerning national cybersecurity strategies or supervisory authorities, are outside the scope.

Third, the geographical scope is limited to Finland. While NIS2 applies across all EU Member States, the national implementation (HE 57/2024) introduces country-specific interpretations and timelines [7]. International companies are defined as those with headquarters outside Finland but with operational presence in Finland; purely domestic Finnish companies are not explicitly analysed, though findings may be transferable. Fourth, the thesis excludes detailed analysis of overlapping regulations such as GDPR, DORA, the EU AI Act, and the Cyber Resilience Act, except where they directly intersect with NIS2 requirements [8]. Fifth, the study does not address sector-specific variations (e.g., manufacturing vs. energy) except where noted in the NIS2 Directive's classification of essential and important entities [3].

Finally, the research is conducted as a qualitative, document-based study without practical case validation. Implementation recommendations are derived from control mapping and literature review, not from live organisational testing. Future empirical research is suggested to validate the proposed model.

1.4 Structure of the Thesis

This thesis is organised into six chapters that progressively build a comprehensive analysis of how international companies in Finland can implement the NIS2 Directive through the ISO/IEC 27001 framework. The first chapter introduces the research by presenting the background and problem statement, outlining the research objectives

and questions, and defining the scope and delimitations of the study. The second chapter provides a literature review, covering the NIS2 Directive's objectives and key requirements, the ISO 27001 framework and ISMS structure, the intersection between regulation and standards, and the identification of the research gap and contribution. The third chapter establishes the theoretical framework, conceptualising compliance through management systems, introducing control mapping as an analytical lens, and proposing a tailored analytical model for NIS2-ISO 27001 alignment. The third chapter describes the research methodology, including the qualitative document-based approach, the systematic control mapping methodology, and a discussion of validity and limitations. The fourth chapter presents the core analysis, mapping NIS2 provisions on risk management, incident reporting, supply chain security onto ISO 27001 controls, and identifying gaps and supplementary measures. The fifth chapter discusses the findings, developing an integrated implementation model, examining practical implications for international companies in Finland, and reflecting on the study's limitations. Finally, the six chapter concludes with a summary of key findings, actionable recommendations for practitioners, and suggestions for future research directions.

2 Literature Review

This chapter reviews the existing literature and official documentation relevant to the implementation of the NIS2 Directive through the ISO/IEC 27001 framework. It begins by examining the NIS2 Directive, detailing its objectives, key cybersecurity requirements (including risk management, incident reporting, and supply chain security), and its transposition into Finnish national legislation via HE 57/2024. The review then turns to the ISO/IEC 27001:2022 framework, outlining its structure as an Information Security Management System (ISMS), its 93 controls organised into four thematic areas, and its emphasis on continuous improvement through the Plan-Do-Check-Act cycle. Subsequently, the chapter explores the intersection between regulation and standards, discussing how internationally recognised frameworks such as ISO 27001 can serve as operational tools for achieving regulatory compliance, and highlighting prior studies that have mapped standards to EU cybersecurity requirements. Finally, the literature review identifies the research gap: while individual mappings of NIS2 to various frameworks exist, a systematic, control-by-control alignment between NIS2 (as implemented in Finland) and ISO/IEC 27001:2022 - including an analysis of gaps and supplementary measures for risk management, incident reporting, and supply chain security - is absent from the current body of knowledge. This chapter thereby establishes the foundation for the theoretical framework and methodological approach that follow.

2.1 The NIS2 Directive: Objectives and Key Requirements

The NIS2 Directive (Directive (EU) 2022/2555) constitutes the European Union's foremost legislative initiative to counter the rising frequency and sophistication of cyberattacks, superseding its predecessor to establish a uniformly high level of cybersecurity across all Member States [3]. Formally adopted in December 2022 and mandated for transposition by 17 October 2024, NIS2 broadens the regulatory scope from 7 to 18 critical sectors, encompassing an estimated 100,000 to 300,000 entities across the Union [10]. The directive introduces stringent incident reporting obligations (an early warning within 24 hours, a detailed notification within 72 hours, and a final report within one month), mandates comprehensive risk management measures under Article 21, requires supply chain security oversight, and holds senior management personally accountable for compliance, with fines reaching up to €10 million or 2% of global annual turnover for essential entities [3], [11], [12].

For the purposes of this thesis, three specific NIS2 provisions are given particular focus due to their complexity and the challenges they pose for international companies operating in Finland.

- Risk management (Article 21) requires entities to adopt a risk-based approach covering policies, network security, vulnerability handling, asset management, access control, encryption, and business continuity [3], [7].

- Incident reporting (Article 23) introduces binding timelines and detailed notification stages, moving beyond the vague and inconsistently applied requirements of the original NIS Directive [3], [13].

- Supply chain security (Article 21(2)(d)) obliges entities to assess risks related to their direct suppliers and service providers, a requirement that is par-

ticularly demanding for international firms with global, multi-tiered supply chains [3], [14].

These three focus areas exemplify the operational and regulatory challenges that international companies face when aligning their existing ISO 27001-based ISMS with NIS2's mandates.

2.1.1 Risk Management (Article 21)

Article 21 of the NIS2 Directive establishes the foundational cybersecurity risk-management obligations for all essential and important entities within the scope [3]. Paragraph 1 requires that Member States ensure these entities take "appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems" [3] used for their operations or services, while also preventing or minimising the impact of incidents on service recipients. The required measures must be based on an "all-hazards approach" and, under paragraph 2, include at least ten enumerated categories [3]:

1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity (including backup management, disaster recovery, and crisis management)
4. Supply chain security
5. Security in network and information systems acquisition, development and maintenance (including vulnerability handling and disclosure)
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
9. Human resources security, access control policies and asset management
10. The use of multi-factor authentication or continuous authentication solutions where appropriate

Paragraph 3 further specifies that entities must consider vulnerabilities specific to each direct supplier and service provider, as well as the overall quality of products and cybersecurity practices of those suppliers, including their secure development procedures [3]. The Commission Implementing Regulation (EU) 2024/2690, adopted on 17 October 2024, lays down the technical and methodological requirements for these risk-management measures for digital infrastructure providers [12], and ENISA has subsequently issued technical guidance to support implementation across all sectors [14].

2.1.2 Incident Reporting (Article 23)

Article 23 of the NIS2 Directive introduces the most prescriptive incident reporting regime ever imposed on network and information system operators across the European Union, replacing the vague and inconsistently applied requirements of the original NIS Directive [3], [14]. Paragraph 1 establishes that each Member State shall ensure that essential and important entities notify their Computer Security Incident Response Team (CSIRT) or competent authority, without undue delay, of any incident that has a significant impact on the provision of their services, while also requiring entities to inform affected service recipients where appropriate [12]. Paragraph 3 defines a "significant incident" as one that has caused, or is capable of causing, either severe operational disruption or financial loss for the entity

concerned, or considerable material or non-material damage to other natural or legal persons [3], [12]. The test is disjunctive - an incident need only meet one of these criteria - and crucially, the language covers both actual and potential impact, meaning organisations cannot wait for harm to materialise before reporting [14]. The Commission Implementing Regulation (EU) 2024/2690, adopted on 17 October 2024, further specifies when an incident shall be considered significant for digital infrastructure providers, including DNS service providers, cloud computing service providers, data centre service providers, and managed service providers, establishing sector-specific thresholds [12].

2.1.3 Supply Chain Security (Article 21(2)(d))

Article 21(2)(d) of the NIS2 Directive explicitly identifies supply chain security as a mandatory element of cybersecurity risk management, requiring essential and important entities to implement appropriate technical, operational and organisational measures that address security-related aspects concerning the relationships between each entity and its direct suppliers or service providers [3], [12]. Paragraph 3 further specifies that entities must consider the vulnerabilities specific to each direct supplier and service provider, as well as the overall quality of products and cybersecurity practices of those suppliers, including their secure development procedures [3]. The NIS2 Directive provides three mechanisms to guarantee supply chain security [3], [12]:

- Coordinated risk assessments carried out at EU level under Article 22
- National risk assessments
- The internal risk assessment obligation under Article 21(2)(d) itself

The Commission Implementing Regulation (EU) 2024/2690, adopted on 17 October 2024, further elaborates supply chain security requirements for digital infrastruc-

ture providers, and ENISA subsequently issued technical implementation guidance that translates these high-level obligations into a 170-page playbook with actionable controls across supply chain security and other domains [12], [14], [15].

2.2 The ISO/IEC 27001 Framework and ISMS Structure

The ISO/IEC 27001 standard is the internationally recognised benchmark for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) [3]. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), it provides a systematic, risk-based framework for managing sensitive information assets through a combination of policies, procedures, and security controls [6]. Certification to the standard is awarded by accredited third-party auditors after a successful Stage 1 (documentation review) and Stage 2 (implementation audit) [16]. The current version, ISO/IEC 27001:2022 [6], represents the most significant update to the standard since 2013 and has been the sole version for new certifications since 31 October 2025 [17].

The ISO 27001 framework is structured into two complementary parts: the main body (Clauses 4 to 10) and Annex A. The main body follows the Annex SL high-level structure, which is shared across all ISO management system standards to facilitate integration with other frameworks such as ISO 9001 (quality management), ISO 22301 (business continuity), and ISO 27701 (privacy management) [6]. These seven mandatory clauses establish the requirements that every organisation must satisfy to achieve certification:

- **Clause 4 (Context of the Organisation)** defines the scope of the ISMS and identifies the needs and expectations of interested parties [6].

- **Clause 5 (Leadership)** requires top management commitment, the establishment of an information security policy, and the definition of clear roles and responsibilities [6].
- **Clause 6 (Planning)** mandates a risk assessment methodology, risk treatment planning, and the definition of measurable information security objectives [6].
- **Clause 7 (Support)** addresses resource allocation, competence and awareness of personnel, communication strategies, and the management of documented information [6].
- **Clause 8 (Operation)** requires the implementation of risk treatment plans and the operational control of security processes [6].
- **Clause 9 (Performance Evaluation)** mandates ongoing monitoring, periodic internal audits, and regular management reviews [6].
- **Clause 10 (Improvement)** covers the handling of nonconformities, corrective actions, and the continual improvement of the ISMS [6].

The 2022 revision introduced several targeted refinements to the main body. Clause 4.2 now requires organisations to identify which interested party requirements will be addressed through the ISMS [6]. Clause 6.2 adds a requirement to monitor information security objectives [6]. Clause 6.3 is entirely new, requiring organisations to plan changes to the ISMS in a structured manner [6]. Clause 8.1 extends operational planning to require criteria for security processes and their control [6]. Organisations are now also required to control "externally provided processes, products or services" relevant to the ISMS, expanding the scope beyond internal processes to include the entire supply chain [6].

The most visible transformation in the 2022 revision is the complete restructuring of Annex A. The previous version contained 114 controls organised across 14 domains; this has been consolidated and reorganised into 93 controls grouped into four thematic categories [6]:

- **Organisational Controls (37 controls)** focus on governance, risk management, policy implementation, asset management, access control, supplier relationships, and incident management, embedding information security into the organisation's culture and strategic decision-making [6].
- **People Controls (8 controls)** address the human element of information security, including screening, terms of employment, awareness training, disciplinary processes, and responsibilities after termination, ensuring that employees understand their security obligations and minimise human-related risks [6].
- **Physical Controls (14 controls)** protect an organisation's infrastructure, facilities, and assets against unauthorised access, theft, and environmental threats, including physical security perimeters, entry controls, equipment security, clear desk policies, and secure disposal [6].
- **Technological Controls (34 controls)** secure digital assets, networks, and IT systems through measures such as authentication, encryption, logging, network security, configuration management, and secure coding, playing a crucial role in preventing unauthorised access and data breaches [6].

The 2022 revision also introduced eleven entirely new controls that reflect the evolving threat landscape, many of which align closely with NIS2 requirements [6], [18]:

1. Threat Intelligence (A.5.7)
2. Information Security for Cloud Services (A.5.23)

3. ICT Readiness for Business Continuity (A.5.30)
4. Physical Security Monitoring (A.7.4)
5. Configuration Management (A.8.9)
6. Information Deletion (A.8.10)
7. Data Masking (A.8.11)
8. Data Leakage Prevention (A.8.12)
9. Monitoring Activities (A.8.16)
10. Web Filtering (A.8.23)
11. Secure Coding (A.8.28)

Each control now includes attributes: control type, information security properties, cybersecurity concepts, operational capabilities, and security domains, facilitating more precise mapping to regulatory requirements [19].

As proposed in this thesis, the ISO 27001 framework serves as a critical operational foundation for achieving NIS2 compliance. The structured, risk-based approach of the ISMS, coupled with the comprehensive control set of Annex A, provides a certifiable and auditable management system that international companies in Finland can leverage to demonstrate adherence to NIS2's twelve risk management measure categories [3], [6]. However, as the analysis in subsequent chapters will demonstrate, gaps remain - particularly in incident reporting timelines, supply chain oversight, and management liability - requiring supplementary measures that extend beyond the scope of ISO 27001 alone [13].

2.3 The Intersection of Regulation and Standards

The relationship between cybersecurity regulations and technical standards has become increasingly interdependent as policymakers seek to translate high-level legal obligations into measurable, auditable practices [20]. Regulations such as the NIS2 Directive, the General Data Protection Regulation (GDPR), and the Digital Operational Resilience Act (DORA) establish mandatory outcomes - for example, "implement appropriate technical and organisational measures" [3] or "ensure the ability to restore operations after an incident" - but typically refrain from prescribing specific technical solutions or management frameworks [3]. This legislative approach, often described as "principle-based regulation," offers flexibility to accommodate sector-specific and organisational contexts but simultaneously creates uncertainty for regulated entities regarding how to demonstrate compliance [13].

Standards, by contrast, provide detailed, tested, and internationally recognised specifications for processes, controls, and management systems [6]. The ISO/IEC 27000 family, the NIST Cybersecurity Framework, and sector-specific standards such as IEC 62443 for industrial automation and control systems offer structured methodologies for risk assessment, control implementation, and continuous improvement [9]. These standards are developed through multi-stakeholder consensus processes and are regularly updated to reflect evolving threats and best practices, making them valuable operational tools for translating regulatory mandates into day-to-day security management [19].

The intersection between regulation and standards manifests in three primary forms. First, regulations may directly reference specific standards as a means of demonstrating conformity. For example, the NIS2 Directive's Commission Implementing Regulation (EU) 2024/2690 explicitly references ISO/IEC 27001, ETSI EN 319 401, and CEN/TS 18026:2024 as examples of standards that can support compliance with technical and methodological requirements [12]. Second, regulators

may recognise certification to a standard as presumptive evidence of compliance with corresponding regulatory provisions, reducing audit burden and providing legal certainty [21]. Third, organisations may voluntarily adopt standards to structure their compliance programmes, even where no direct regulatory mandate exists, as a means of demonstrating due diligence and risk-based decision-making [22].

The alignment of an Information Security Management System (ISMS) with an internationally recognised standard such as ISO 27001 offers several advantages for navigating complex regulatory landscapes. A standard-based ISMS provides a documented, repeatable, and auditable framework that covers risk management, asset control, incident handling, business continuity, and supplier oversight - all of which are recurring themes across multiple EU regulations [23]. By adopting a single ISMS that is designed to be extensible, organisations can avoid the inefficiency of maintaining separate compliance silos for NIS2, GDPR, DORA, and other overlapping requirements [19]. This approach, sometimes referred to as "integrated compliance," relies on the principle that a well-designed management system can be mapped to multiple regulatory frameworks through a common set of controls, with supplementary measures added only where specific regulatory obligations exceed the standard's scope [13].

However, the intersection between regulation and standards is not without challenges. Standards are developed independently of regulatory cycles [5], meaning that a standard may not fully address the most recent regulatory updates. Conversely, regulations may reference standards that have since been revised, creating versioning mismatches. Organisations must therefore maintain current mappings between their chosen standards and applicable regulations, a process that requires ongoing monitoring and periodic reassessment [24]. Additionally, the language of standards is often permissive ("should" rather than "shall"), whereas regulations use mandatory language, necessitating careful interpretation to ensure that alignment claims

are substantiated [13].

For international companies operating in Finland, the intersection of NIS2 with ISO 27001 represents a strategic opportunity. The directive's twelve risk management measure categories correspond broadly to the structure of an ISMS, and the standard's 2022 revision introduced controls - such as threat intelligence, cloud security, and ICT business continuity - that directly address modern cyber risks [3], [6]. By designing an ISMS that is explicitly aligned with NIS2's provisions while remaining flexible for future regulatory developments [13], organisations can transform compliance from a reactive burden into a strategic enabler of cyber resilience. The subsequent chapters of this thesis will develop a systematic methodology for achieving such alignment, demonstrating how a well-structured ISMS can serve as the operational backbone for multi-regulatory compliance in the Finnish context.

2.4 Research Gap and Contribution

To establish the research gap, a systematic literature search was conducted across different major academic databases: IEEE Xplore, Google Scholar, ACM Digital Library, ScienceDirect, and Wiley Online Library. The following keyword combinations were used: (1) "NIS2" AND "ISO 27001" AND "compliance"; (2) "NIS2" AND "control mapping"; (3) "NIS2" AND "Finland" AND "implementation"; (4) "cybersecurity regulation" AND "ISO 27001" AND "gap analysis"; and (5) "NIS2" AND "risk management" AND "incident reporting" AND "supply chain security". The search was limited to peer-reviewed articles, conference proceedings, and official technical reports published between 2018 and 2025. The search returned few direct matches: most results were either high-level overviews of the NIS2 Directive without technical depth, or generic discussions of ISO 27001 implementation without specific reference to NIS2. No studies were found that provided a systematic, control-by-control mapping between NIS2 (as transposed into Finnish law)

and ISO/IEC 27001:2022 with an analysis of gaps and supplementary measures. Semi-related articles - such as those discussing GDPR compliance through ISO 27001, or sector-specific NIS2 interpretations for energy or finance - were identified and are discussed below to illustrate the boundaries of existing research.

Despite the growing body of literature on the NIS2 Directive and the widespread adoption of ISO/IEC 27001 as a cybersecurity management framework, several significant gaps remain in both academic research and practical guidance.

First, systematic control-level mappings are lacking. While Vandezande (2024) [13] provides a comprehensive legal analysis of the NIS2 Directive and its differences from the original NIS Directive, the study does not extend to a technical control-by-control mapping between NIS2's twelve risk management measure categories and ISO 27001's 93 controls. Similarly, Monica et al. (2021) [24] examine the implementation challenges of the original NIS Directive across Member States but stop short of providing a granular alignment with any standard. Existing industry resources, such as the ENISA NIS2 Technical Implementation Guidance (2025) [14], offer high-level recommendations ("ISO 27001 can support compliance") but do not identify which specific Annex A controls address which NIS2 provisions. Sector-specific studies (e.g., energy or finance) [25], [26] provide partial mappings but lack the cross-sectoral applicability needed for international companies operating across multiple industries in Finland.

Second, operational integration has not been addressed. While scholars such as Mettler (2011) [22] and Song et al. (2024) [23] have discussed maturity models and risk management frameworks in general, no empirical or design-based study provides a step-by-step methodology for extending an existing ISO 27001-certified ISMS to cover NIS2-specific requirements. The 24-hour incident reporting timeline, explicit supply chain due diligence obligations, and personal management liability provisions are not adequately addressed in existing ISO 27001 implementation guides. Prac-

titioners therefore rely on fragmented, vendor-driven guidance - such as checklists from consulting firms - that lack academic validation and generalisability [18], [27].

Third, the Finnish national context has received minimal attention. Although the Finnish government has published a detailed national implementation proposal (HE 57/2024) [7] and the National Cyber Security Centre Finland (NCSC-FI) has developed the Kybermittari maturity assessment tool [28], no peer-reviewed study has systematically examined how international companies operating under Finnish jurisdiction can leverage ISO 27001 to meet both EU-level and Finnish-specific requirements. Existing theses, such as those by Bowo (2025) [29] and Fransila (2024) [30], focus on maturity assessments or company-specific implementation projects but do not provide a generalisable, control-by-control mapping. This gap is particularly problematic given Finland's high digital maturity and the presence of numerous international firms in manufacturing, digital infrastructure, and energy sectors that fall under NIS2's scope.

Fourth, an integrated implementation model is missing. While some resources provide checklists (e.g., "implement ISO 27001 and you will be compliant") or overly technical control mappings that lack strategic guidance on governance, documentation, and audit preparation, no validated model combines control mapping with practical implementation steps and gap remediation strategies. Studies such as those by Trent (2023) [31] and Suksi (2025) [32] address compliance in specific domains (marine and IoT) but do not offer a comprehensive framework applicable to the broad range of international companies in Finland.

In response to these gaps, this thesis makes the following contributions:

1. It provides a systematic, control-by-control mapping between the NIS2 Directive (as implemented in Finland via HE 57/2024) and ISO/IEC 27001:2022, with particular emphasis on the three most challenging provisions: risk management (Article 21), incident reporting (Article 23), and supply chain security

(Article 21(2)(d)).

2. It identifies and categorises gaps where ISO 27001 controls fall short of NIS2 requirements, and proposes specific supplementary measures to address those gaps.

3. It develops an integrated, step-by-step implementation model that international companies in Finland can use to extend their existing ISMS for NIS2 compliance, including guidance on documentation, internal audit, and management review.

4. It synthesises findings into actionable recommendations for practitioners, policymakers, and future researchers, thereby bridging the divide between regulatory mandates and operational reality.

By delivering these contributions, this aims to accomplish the **RO1**, **RO2**, and **RO3** and ultimately aims to serve as a practical reference for international companies seeking to transform NIS2 compliance from a regulatory burden into a strategic component of their cybersecurity management system.

3 Research Methodology

This chapter presents the research methodology employed to address the two research questions formulated in Chapter 1. The study adopts a mixed-methods research design that combines doctrinal legal research, comparative analysis, and content analysis, culminating in a critical framework evaluation that directly supports **RQ2**. First, doctrinal legal research is applied to systematically interpret the binding legal requirements of the NIS2 Directive (EU 2022/2555) and their transposition into Finnish national legislation via HE 57/2024 [7], establishing a precise, article-by-article specification of what regulated entities must achieve. This step addresses the regulatory-interpretive dimension of **RQ1** (how ISO 27001 can be mapped and utilised). Second, comparative analysis is conducted to juxtapose the identified NIS2 requirements against the 93 controls of ISO/IEC 27001:2022, identifying direct alignments, partial overlaps, and complete gaps. This comparative phase also provides the empirical basis for answering **RQ1** by revealing which ISO controls can be leveraged for each NIS2 provision. Third, content analysis is performed on the text of the directive, the Finnish implementation act, and the ISO 27001:2022 standard to extract not only explicit obligations but also implicit expectations, such as the required rigour of risk assessments or the evidentiary standards expected by supervisory authorities. The output of these three analytical strands feeds directly into a critical framework evaluation, which constitutes the core of **RQ2**: assessing the strengths, limitations, and identified gaps when employing ISO 27001 controls

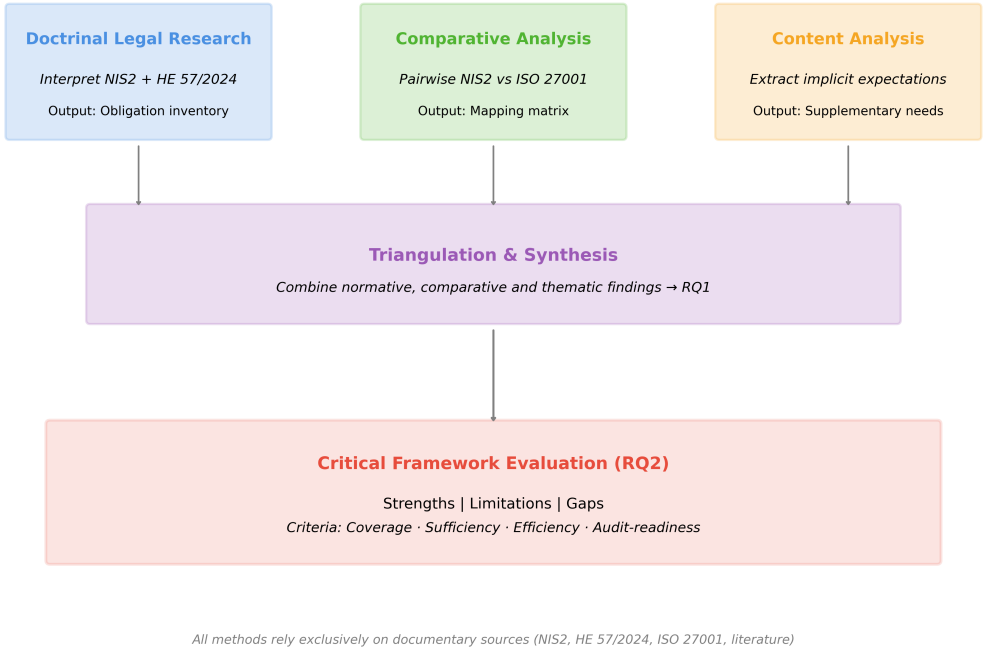
for NIS2 compliance. This evaluation goes beyond mere mapping by weighing the sufficiency, efficiency, and audit-readiness of an ISO 27001-based ISMS in the specific context of international companies operating in Finland. The following sub-sections detail the research approach, the document analysis and control mapping methodology, and the validity and limitations of the chosen methods.

3.1 Research Approach

The methodological foundation of this thesis rests on a qualitative, interpretivist paradigm, chosen because the study investigates how legally binding norms (the NIS2 Directive and its Finnish transposition) intersect with a voluntary technical benchmark (ISO/IEC 27001:2022) within the operational settings of internationally owned enterprises based in Finland [33]. Two core research questions drive the inquiry, and to answer them the study employs a tripartite qualitative strategy that integrates doctrinal legal analysis, comparative assessment, and thematic content extraction, followed by an evaluative synthesis. Figure 3.1 provides a visual overview of this stepwise mixed-methods design, showing how the three parallel analytical strands feed into a central synthesis and ultimately into the critical framework evaluation.

The first strand, doctrinal legal research, systematically unpacks the enforceable duties imposed by the NIS2 Directive (left column of Figure 3.1). Attention centres on Articles 21 (risk management), 23 (incident reporting) and 21(2)(d) (supply chain security), alongside their domestication into Finnish law through the government proposal HE 57/2024 [3], [7]. This type of legal analysis goes beyond a plain reading of the text: it considers recitals, preparatory documents, and the overarching legislative purpose, thereby constructing a detailed normative yardstick. The outcome directly supports the first research question **RQ1** by defining precisely what "comprehensive compliance" entails from a legal-technical standpoint.

Figure 3.1: Research Approach Overview Visualization



The second strand consists of comparative analysis, which places the previously identified NIS2 obligations alongside the control set of ISO/IEC 27001:2022 (middle column of Figure 3.1). Each regulatory requirement - for instance, "deploy multi-factor authentication where circumstances warrant it" - is compared with the corresponding ISO control (e.g., A.5.17 Authentication information) and assessed for the degree of correspondence: full alignment, partial overlap, or no coverage [6], [13]. This comparison is carried out at a granular, control-by-control level and is organised around the thesis's three focal areas (risk management, incident reporting, supply chain security). The output provides the empirical backbone for addressing the first research question **RQ1**.

The third strand, content analysis, examines the textual substance of both the NIS2 Directive and the ISO 27001:2022 standard in a more interpretive manner (right column of Figure 3.1). Unlike doctrinal analysis, which focuses on legal norms, content analysis surfaces implicit themes, hidden expectations, and evidentiary requirements that are not stated outright yet are critical for practical compliance [34].

For example, while the directive speaks of "policies to assess the effectiveness of cybersecurity measures," a content-analytic reading reveals that supervisory bodies anticipate documented proof of periodic management reviews coupled with measurable performance indicators. This layer of interpretation closes the gap between legislative wording and audit-room reality.

The findings from the three analytical strands converge in a critical framework evaluation, which directly tackles the second research question **RQ2** concerning the strengths, weaknesses, and gaps of ISO 27001 when used for NIS2 compliance. This convergence is represented by the "Triangulation & Synthesis" and "Critical Framework Evaluation" stages in the lower part of Figure 3.1. The evaluation applies a multi-criteria lens derived from both the legal requirements and the hallmarks of an effective ISMS: coverage (does the control meet the obligation?), sufficiency (is the control alone enough, or are add-ons required?), efficiency (can it be implemented without disproportionate cost or effort?), and audit-readiness (does it generate verifiable, auditable evidence?) [22], [23]. The evaluation does not assume that ISO 27001 is either flawless or inadequate; instead, it pinpoints areas where the standard performs well (e.g., structured risk assessment) and areas that demand supplementary measures (e.g., the 24-hour incident notification timeline).

All three methods rely exclusively on documentary sources, as indicated in the bottom annotation of Figure 3.1. These include primary legal materials (the NIS2 Directive, HE 57/2024 [7], Commission Implementing Regulation (EU) 2024/2690), the technical standard ISO/IEC 27001:2022, and peer-reviewed academic literature. No primary data collection - such as interviews, surveys, or organisational case studies - is undertaken. This documentary-only design ensures that the resulting mapping and evaluation are generalisable and can be applied by any international company in Finland without access to confidential internal data [35]. The qualitative, interpretivist stance is well suited to the exploratory and analytical aims of

the thesis and mirrors established approaches in the field of cybersecurity regulation and standard alignment [13], [22].

The following sub-sections elaborate the concrete steps for document analysis and control mapping (Section 3.2), followed by a transparent discussion of validity considerations and methodological limitations (Section 3.3).

3.2 Document Analysis and Control Mapping Methodology

This section details the concrete procedures used to extract, compare, and synthesise information from the primary documents. The methodology follows a structured, replicable workflow consisting of five sequential phases: (i) document sampling and preparation, (ii) extraction of normative requirements from NIS2 and HE 57/2024 [7], (iii) extraction of control statements from ISO/IEC 27001:2022, (iv) pairwise mapping and gap classification, (v) supplementary mapping for Finnish national specificities, and (vi) documentation and replicability. Figure 3.2 provides a visual overview of this entire six-step process, from document sampling through to the final output matrix, including the parallel extraction steps and the supplementary mapping for Finnish specificities.

3.2.1 Document Sampling and Preparation

The document corpus was deliberately limited to sources that carry binding or authoritative weight for international companies subject to NIS2 supervision in Finland. Three document categories were included. The first category comprises the NIS2 Directive (EU 2022/2555) itself, specifically Articles 21 (risk management measures), 23 (incident reporting), and the corresponding recitals that provide interpretive context, as well as the Commission Implementing Regulation (EU) 2024/2690,

Figure 3.2: Document Analysis and Control Mapping Methodology Diagram

which adds technical specifications for digital infrastructure providers [3], [12]. The second category is the Finnish government proposal HE 57/2024 [7], which transposes the directive into national law and supplies the twelve risk management measure categories that supervisory authorities will use during inspections [7]. The third category is the full text of ISO/IEC 27001:2022, including Clauses 4-10 and all 93 Annex A controls [6]. All documents were accessed in their official English versions (where available) to ensure terminological consistency. Each document was converted into a plain-text format and scrutinized thoroughly for qualitative data

analysis to facilitate systematic coding. As shown in the top box of Figure 3.2, this step results in a defined and version-controlled document corpus.

3.2.2 Extraction of NIS2 Requirements

A doctrinal reading of the NIS2 Directive and HE 57/2024 was performed to identify every distinct obligation expressed using mandatory language ("shall," "must," "is required to"). Each obligation was recorded as a separate requirement statement and tagged with three attributes: (a) the article or section number, (b) the specific focus area (risk management, incident reporting, or supply chain security), and (c) the level of prescriptiveness (exact specification, principle-based direction, or optional guidance). For example, Article 23(4) of NIS2 stating "the entity shall submit an early warning within 24 hours" was captured as a precise, time-bound obligation, whereas Article 21(2)(b) requiring "appropriate measures regarding incident handling" was recorded as a principle-based obligation that leaves room for interpretation [3]. This extraction yielded a structured inventory of NIS2 requirements that served as the left-hand column of the subsequent mapping matrix. This phase corresponds to the left-hand box in Figure 3.2, labelled "3.2.2 Extraction of NIS2 Requirements".

3.2.3 Extraction of ISO 27001 Control Statements

A parallel extraction was performed on ISO/IEC 27001:2022. Instead of taking the standard's own grouping (organisational, people, physical, technological), each Annex A control was transcribed verbatim and then summarised in plain operational language to facilitate comparison. For instance, control A.5.24 ("information security incident management planning and preparation") was summarised as "the organisation shall establish documented incident management plans, procedures and responsibilities before any incident occurs" [6]. Clause-level requirements

(e.g., Clause 6.1 on risk assessment and treatment) were also extracted because they impose process obligations that complement Annex A controls. Each extracted statement was tagged with its unique control or clause identifier and its thematic area (governance, incident response, continuity, supplier management, etc.). This parallel extraction step is visualised in the right-hand box of Figure 3.2, labelled "3.2.3 Extraction of ISO 27001 Controls".

3.2.4 Pairwise Mapping and Gap Classification

The core of the methodology is a pairwise mapping between each NIS2 requirement and the ISO 27001 controls. For each NIS2 requirement, the following question was asked: "Does ISO 27001:2022 contain a control or clause that, when implemented, would satisfy this requirement in whole or in part?" Where a direct match was identified (e.g., NIS2 Article 21(2)(j) on multi-factor authentication mapping to ISO 27001 A.5.17), it was recorded as a full alignment. Where the requirement was partially addressed but left gaps (e.g., NIS2's 24-hour reporting timeline versus ISO 27001's "as quickly as possible" language in control A.5.25), the pair was recorded as partial overlap with a note on the missing element. Where no relevant control could be found (e.g., NIS2's requirement that management bodies "be held liable for infringements" has no equivalent in ISO 27001), the requirement was flagged as a complete gap. To ensure consistency, a four-point coding scheme was used: "F" (full - the ISO control entirely covers the NIS2 requirement), "P" (partial - some but not all elements covered), "G" (gap - no coverage), and "N/A" (not applicable - the NIS2 requirement addresses a purely supervisory matter outside the ISMS scope). The student author performed all mapping decisions and recorded them in a structured matrix table, which is presented in Appendix A of the thesis and serves as the empirical foundation for the analysis in Chapter 4. The mapping process was iterative: when a NIS2 requirement appeared to map to more than one

ISO control, all relevant controls were listed, and the combination was assessed for sufficiency. The output is a transparent, auditable traceability link between regulatory text and standard controls. This central mapping activity is depicted in the middle of Figure 3.2 under "3.2.4 Pairwise Mapping & Gap Classification".

3.2.5 Supplementary Mapping for Finnish National Specificities

As this thesis focuses on international companies in Finland, an additional mapping step was added. The twelve risk management measure categories listed in HE 57/2024 [7] were extracted and compared against the same ISO 27001 controls. While these categories largely mirror NIS2 Article 21, the Finnish proposal adds national-level interpretation notes (e.g., specifying that "secure development" includes mandatory vulnerability disclosure processes). Any category that introduced a requirement exceeding the plain text of the NIS2 Directive was flagged and, where necessary, cross-referenced to Finnish guidance documents [28] (e.g., NCSC-FI recommendations) to identify supplementary measures not found in ISO 27001. This step ensures that the final implementation model is tailored to the Finnish supervisory landscape. Figure 3.2 shows this step as "3.2.5 Supplementary Mapping for Finnish Specificities", placed after the main pairwise mapping to reflect its role in adapting the generic alignment to the Finnish context.

3.2.6 Documentation and Replicability

All extraction sheets, mapping matrices, and coding decisions were stored in a research log maintained by the student author. The entire procedure is designed to be replicable by other researchers or practitioners using the same document versions. Any future update to NIS2 (e.g., further implementing acts) or to ISO 27001 would require the mapping to be repeated, but the methodological steps described here

would remain unchanged. The final box in Figure 3.2, labelled "3.2.6 Documentation & Replicability", summarises this commitment to transparency and reproducibility, and the arrow leads to the output matrix (Appendix A) at the bottom of the figure.

3.3 Validity and Limitations

This section briefly discusses the trustworthiness of the study's findings and acknowledges the inherent constraints of the chosen methodology.

3.3.1 Validity

To ensure **internal validity** (that the mapping truly reflects the relationship between NIS2 and ISO 27001), the student author applied a systematic, consistent coding scheme and documented all mapping decisions in a research log. **External validity** (generalisability) is supported because the core NIS2-ISO 27001 mapping applies across EU Member States, while a separate step adapts the model to Finland's national legislation (HE 57/2024) [7]. **Construct validity** was addressed by using well-defined coding categories (full, partial, gap) drawn from prior literature [13], [23]. **Reliability** (replicability) is ensured through detailed documentation of all steps, the research log, and the mapping matrix provided in Appendix A, allowing another researcher to repeat the procedure with the same document versions.

3.3.2 Limitations

Several limitations should be noted. First, the study uses only documentary sources (laws, standards, literature) and no empirical data from real organisations; therefore, the findings are normative, not descriptive of actual practice. Second, the mapping is static and tied to the 2022 versions of NIS2 and ISO 27001; future updates may require revision. Third, some classification decisions involve interpretation (e.g.,

principle-based requirements), though the student author mitigated this by using explicit coding criteria and documenting all decisions. Fourth, the study does not assess the cost or proportionality of the recommended supplementary measures, leaving that to practitioners. Fifth, the analysis focuses exclusively on ISO 27001; other frameworks are not compared. Sixth, the proposed implementation model remains conceptual until validated by future empirical research (e.g., case studies). These limitations do not undermine the study's objectives but should be kept in mind when applying the results.

4 Analysis: Mapping NIS2 to ISO 27001

This chapter presents the core empirical analysis of the thesis, systematically examining the alignment between the NIS2 Directive (Articles 21 and 23, with particular emphasis on risk management, incident reporting, and supply chain security) and the control set of ISO/IEC 27001:2022. The analysis follows the methodological framework described in Chapter 3, applying doctrinal legal interpretation, comparative assessment, and content analysis to produce a granular, control-by-control mapping. For each of the three focal areas - risk management (Section 4.1), incident handling and reporting (Section 4.2), and supply chain security (Section 4.3) - the chapter identifies whether ISO 27001 controls fully satisfy the corresponding NIS2 obligation, partially cover it, or leave a complete gap. Where partial coverage or gaps exist, the analysis explains the nature of the deficiency and flags the need for supplementary organisational measures. Section 4.4 then synthesises the findings into a consolidated list of gaps and proposes targeted supplementary measures that international companies operating in Finland must adopt to bridge the remaining distance between an ISO 27001-based Information Security Management System (ISMS) and full NIS2 compliance. The mapping tables summarised in Appendix A provide the detailed evidence base for the conclusions drawn in this chapter, drawing on the NIS2 Directive [3], the ISO/IEC 27001:2022 standard [6], and the Finnish

national implementation proposal HE 57/2024 [7].

4.1 Risk Management Requirements

Article 21 of the NIS2 Directive establishes the foundational cybersecurity risk-management obligations for essential and important entities [3]. Paragraph 2 enumerates ten distinct measures, ranging from risk analysis policies and incident handling to business continuity, supply chain security, access control, and the use of multi-factor authentication. Paragraph 3 adds a specific requirement concerning vulnerability assessments of each direct supplier. The systematic mapping of these provisions onto ISO/IEC 27001:2022 is presented in Table A.1 of Appendix A, with each classification denoted as **F** (full alignment), **P** (partial overlap), or **G** (gap). This section interprets the mapping results thoroughly to justify the research objectives. The mapping reveals that the majority of NIS2 Article 21 requirements are fully addressed by ISO 27001:2022, while three areas require supplementary measures.

4.1.1 Full Alignments (F)

The following provisions of Article 21 are fully satisfied by implementing the corresponding ISO 27001 controls as written, without the need for modification:

i) **21(2)(a) - Policies on risk analysis and information system security**

ISO 27001 controls A.5.1 (policies for information security), A.5.8 (information security in project management), and Clause 6.1 (actions to address risks) mandate management-approved documented security policies and a formal risk assessment process [6]. Organisations with a certified ISMS already meet this requirement fully.

ii) **21(2)(d) - Supply chain security**

Controls A.5.19 (supplier relationships), A.5.20 (supplier agreements), and A.5.21 (ICT supply chain management) collectively require supplier risk identification, contractual security obligations, and ongoing monitoring of ICT supply chain risks. This triad directly mirrors NIS2's expectations for direct supplier management.

iii) **21(2)(e) - Security in acquisition, development, maintenance and vulnerability handling**

Multiple controls - A.5.14 (secure development), A.5.8 (project management), A.8.25 (secure development life cycle), and A.8.8 (management of technical vulnerabilities) - cover the entire lifecycle. Vulnerability handling (A.8.8) explicitly includes disclosure processes, fully aligning with NIS2.

iv) **21(2)(f) - Policies to assess effectiveness of cybersecurity risk-management measures**

Clause 9.1 (monitoring, measurement, analysis, evaluation), Clause 9.2 (internal audit), and Clause 9.3 (management review) embed the Plan-Do-Check-Act (PDCA) cycle, requiring regular effectiveness assessments, internal audits, and management reviews - a complete match.

v) **21(2)(g) - Basic cyber hygiene and cybersecurity training**

Controls A.6.3 (information security awareness, education, training) and A.5.36 (compliance with policies) mandate ongoing awareness programmes and verification of policy adherence, covering hygiene and training obligations.

vi) **21(2)(h) - Policies on cryptography and encryption**

Controls A.5.31 (legal, regulatory and contractual requirements - encryption aspects) and A.8.24 (use of cryptography) require a documented cryptographic

policy, key management, and appropriate encryption use, fully satisfying NIS2.

vii) **21(2)(i) - Human resources security, access control, asset management**

A comprehensive set of controls - A.5.9 (asset inventory), A.5.15 (access control), A.5.16 (identity management), A.5.17 (authentication information), A.5.18 (access rights), and the entire Clause 6 people controls (A.6.1 to A.6.8) - provides exhaustive coverage of asset management, access governance, and human-centric security measures (screening, responsibilities, disciplinary processes).

4.1.2 Partial Alignments (P)

The following provisions require supplementary measures because ISO 27001 provides a procedural foundation but lacks specific NIS2 mandates:

i) **21(2)(b) - Incident handling** Controls A.5.24, A.5.25, and A.5.26 establish the incident management lifecycle (preparation, detection, assessment, response, learning). **Gap:** ISO 27001 states that incidents shall be reported "as quickly as possible," whereas NIS2 mandates binding timelines: an early warning within 24 hours, a detailed notification within 72 hours, and a final report within one month [3]. **Supplementary measure:** a dedicated NIS2 incident notification protocol with tracked deadlines.

ii) **21(2)(c) - Business continuity, backup, disaster recovery, crisis management** Control A.5.30 (ICT readiness for business continuity, added in the 2022 revision) and A.5.29 (information security during disruptions) align well with continuity requirements. **Gap:** NIS2 explicitly lists "crisis management" as a separate element; ISO 27001 addresses crisis response only indirectly under A.5.29. **Supplementary measure:** a dedicated crisis communication

and management protocol.

iii) **21(2)(j) - Multi-factor authentication or continuous authentication** Controls A.5.17 (authentication information) and A.8.5 (secure authentication) require secure authentication but allow discretion ("where appropriate"). NIS2 is more prescriptive, expecting MFA as a default for remote access and sensitive systems. **Supplementary measure:** a stricter internal MFA policy that removes the "where appropriate" discretion and mandates MFA in all relevant scenarios.

iv) **21(3) - Supply chain vulnerability assessment (each direct supplier)** Controls A.5.19-A.5.21 and Clause 8.1 (operational planning for external providers) address supplier risk assessment. **Gap:** ISO 27001's risk-based approach does not explicitly require an individual vulnerability assessment for each direct supplier, whereas NIS2's phrasing ("vulnerabilities specific to each direct supplier") implies greater granularity. **Supplementary measure:** enhance supplier assessment templates to document per-supplier vulnerabilities, especially for critical or high-risk providers.

4.1.3 No Alignments (G)

None of the risk management provisions in Article 21 are completely uncovered. Every measure has at least partial coverage. However, the binding timeline for incident notification is not a control gap but a procedural gap, as noted above.

In summary, ISO 27001:2022 provides an excellent foundation for NIS2 Article 21, with full alignments covering approximately 63.6% of the requirements. The remaining partial gaps are narrow and remediable through targeted supplementary procedures - predominantly in the areas of incident reporting timelines, crisis management specificity, MFA prescriptiveness, and supplier vulnerability granularity.

Figure 4.1: Bar Chart Representation of NIS2 Risk Management Requirements - Alignment with ISO/IEC 27001:2022

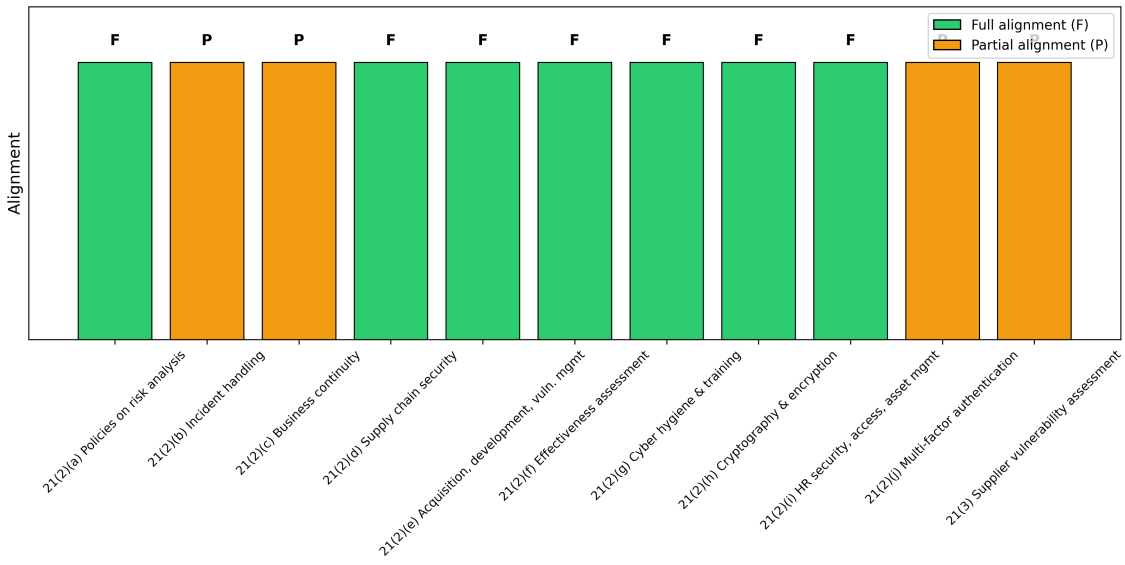
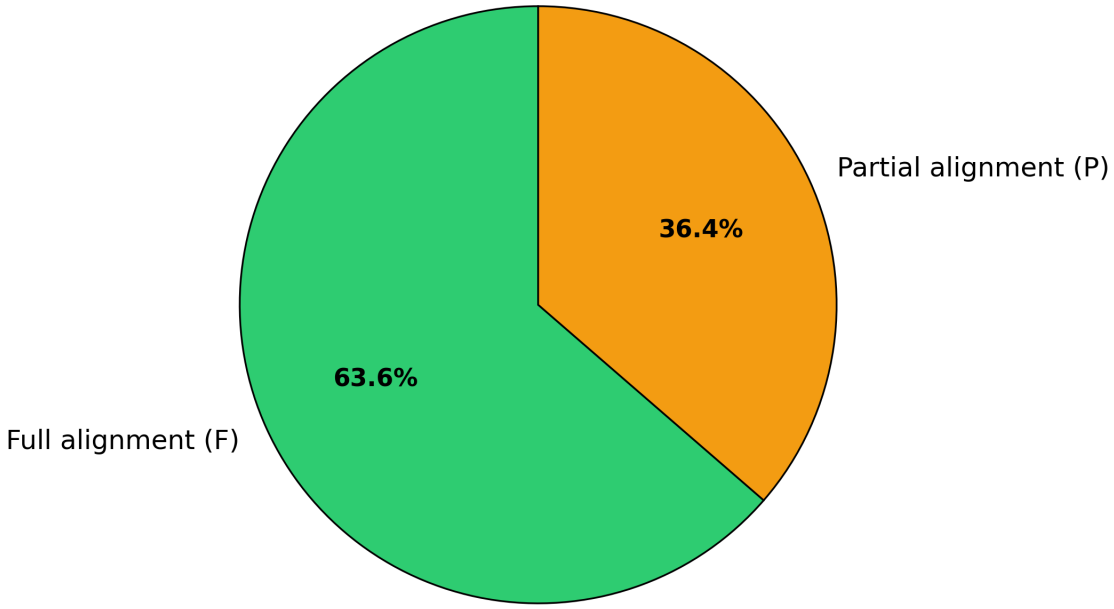


Figure 4.2: Proportion of Full vs. Partial Alignments (NIS2 Article 21)



None of these gaps require abandoning or fundamentally restructuring an existing ISMS. Section 4.4 consolidates these gaps and proposes actionable supplementary

measures.

4.2 Incident Handling and Reporting

Article 23 of the NIS2 Directive introduces the most prescriptive incident reporting regime imposed on network and information system operators across the European Union [3]. Unlike its predecessor, which allowed Member States broad discretion, Article 23 establishes binding timelines (early warning within 24 hours, detailed notification within 72 hours, and a final report within one month), a clear definition of a "significant incident" (severe operational disruption, financial loss exceeding €500,000, or material damage), and mandatory notifications to both competent authorities and affected service recipients [3], [12]. The mapping of these provisions onto ISO/IEC 27001:2022 is summarised in Table A.2 of Appendix A, revealing that while the ISO standard provides a strong internal incident management framework, it leaves critical gaps concerning external reporting timelines and notification formats. The mapping shows that ISO 27001:2022 partially covers three requirements, fully covers none, and leaves two requirements completely uncovered.

4.2.1 Partial Alignments (P)

i) **23(3) - Definition of "significant incident" (severe operational disruption, financial loss, material damage)**

ISO 27001 control A.5.25 (assessment and decision on information security events) requires the organisation to classify events as incidents based on predefined criteria. **Gap:** The standard does not prescribe the quantitative thresholds (e.g., financial loss > €500,000) or the qualitative criteria (e.g., "severe operational disruption") used by NIS2. Organisations must therefore adopt the NIS2 significance thresholds into their internal incident classifica-

tion scheme. **Supplementary procedure:** amend the incident classification matrix to incorporate the exact NIS2 criteria, and train personnel on applying them consistently.

ii) **23(4)(c) - Final report within one month (root cause, mitigation, cross-border impact)**

ISO 27001 control A.5.26 (response to information security incidents) and Clause 10.1 (nonconformity and corrective action) require root cause analysis, corrective actions, and documented lessons learned. **Gap:** ISO 27001 does not mandate a final report to an external CSIRT or competent authority, nor does it specify a one-month deadline. The content (root cause, mitigation) is covered, but the external reporting format and timeline are not. **Supplementary procedure:** establish a formal final report template that includes root cause, applied mitigations, and cross-border impact, and enforce the one-month submission deadline.

iii) **23(2) - Notify affected service recipients of significant cyber threats and remediation measures**

ISO 27001 control A.7.4 (communication with specific interest groups) provides a framework for external communication but does not specifically require notifying recipients of a cyber threat or prescribing the content of such notification. **Gap:** The standard leaves the decision to communicate up to the organisation, whereas NIS2 mandates notification "without undue delay." **Supplementary procedure:** develop a standardised customer/recipient notification template and embed it into the incident response playbook.

4.2.2 No Alignments (G)

i) **23(4)(a) - Early warning within 24 hours (including malicious act suspicion and cross-border impact)**

ISO 27001 contains no binding timeline for initial notification. The standard's wording ("as quickly as possible" in control A.5.25) is not equivalent to 24 hours. Moreover, the requirement to indicate whether the incident is suspected of being caused by unlawful or malicious acts, and whether it could have a cross-border impact, is absent from ISO 27001. **Supplementary measure:** implement a dedicated early-warning procedure that triggers within 24 hours of becoming aware of the incident, including a checklist for malicious act suspicion and cross-border implications.

ii) **23(4)(b) - Incident notification within 72 hours (severity, impact, indicators of compromise)**

ISO 27001 does not specify a 72-hour detailed notification to an external authority. The standard's communication clauses (Clause 7.4) are generic and do not prescribe submission of severity assessments, impact analyses, or IoCs to a CSIRT. **Supplementary measure:** develop a structured incident notification template that captures severity, impact assessment, and known IoCs, and ensure it is submitted to the competent authority within 72 hours of the early warning.

In summary, ISO 27001:2022 provides a sound internal incident management process but is wholly inadequate for meeting NIS2's external reporting timelines and formats. The standard's "as quickly as possible" language is not legally enforceable against the directive's 24-hour and 72-hour deadlines. Organisations cannot rely on their existing ISMS alone for incident reporting compliance. Instead, they must overlay a dedicated NIS2 notification procedure that includes:

1. 24-hour early warning template with malicious act and cross-border checks
2. A 72-hour detailed notification template with severity, impact, and IoCs
3. A one-month final report template with root cause, mitigation, and cross-border impact, and
4. A mandatory customer/recipient notification process

These supplementary measures are elaborated in Section 4.4.

4.3 Supply Chain Security

Article 21(2)(d) and Article 21(3) of the NIS2 Directive place explicit and detailed obligations on entities to manage cybersecurity risks arising from their supply chains. Paragraph 2(d) requires entities to address security-related aspects concerning relationships with their direct suppliers or service providers, while paragraph 3 goes further by mandating that entities consider vulnerabilities specific to each direct supplier, the overall quality of products, and the cybersecurity practices of those suppliers, including their secure development procedures [3]. The mapping of these provisions onto ISO/IEC 27001:2022 is presented in Table A.3 of Appendix A, which classifies one requirement as a full alignment and one as a partial overlap. The mapping shows that ISO 27001:2022 fully aligns with one requirement and partially aligns with the other. No complete gaps are present in the supply chain security domain.

4.3.1 Full Alignment (F)

21(2)(d) - Address security-related aspects concerning relationships with direct suppliers or service providers

ISO 27001 controls A.5.19 (supplier relationships), A.5.20 (supplier agreements), and A.5.21 (ICT supply chain management) collectively require organisations to: (a) define and implement processes to manage risks associated with supplier access to the organisation's information assets; (b) establish and document supplier agreements that include information security requirements; (c) monitor and review supplier service delivery; and (d) manage risks specifically arising from the ICT supply chain (e.g., hardware, software, and services). These three controls directly mirror NIS2's expectations for addressing security aspects of direct supplier relationships. Organisations with a certified ISMS that implements these controls fully satisfy Article 21(2)(d) without supplementary measures.

4.3.2 Partial Alignment (P)

21(3) - Consider vulnerabilities specific to each direct supplier, product quality, and cybersecurity practices (including secure development procedures)

The same ISO 27001 controls (A.5.19-A.5.21) address supplier risk assessment and ICT supply chain management at a general level. However, NIS2 Article 21(3) introduces a higher degree of granularity. **Gap:** The ISO standard's risk-based approach typically allows organisations to categorise suppliers by criticality and perform risk assessments proportionally. It does not explicitly require an individual vulnerability assessment for each direct supplier - especially for low-risk or non-critical suppliers - nor does it mandate that organisations assess the quality of products and the security development practices of each supplier. NIS2's phrasing ("vulnerabilities specific to each direct supplier") implies a supplier-by-supplier analysis

that may exceed the standard's conventional scope. **Supplementary measure:** Enhance the supplier risk assessment template to explicitly document, for every direct supplier, (i) identified vulnerabilities specific to that supplier, (ii) an evaluation of the supplier's product quality, (iii) a review of the supplier's secure development procedures (where applicable), and (iv) a risk rating based on this granular analysis. For suppliers deemed critical, this assessment should be conducted at least annually and prior to contract renewal.

ISO 27001:2022 provides a robust foundation for supply chain security, fully covering the general obligation to manage supplier relationships (21(2)(d)). The only gap concerns the explicit requirement to assess each direct supplier individually for vulnerabilities and product quality (21(3)). This gap is narrow and remediable: organisations need only to supplement their existing supplier management process with a more granular, per-supplier vulnerability assessment checklist. No major restructuring of the ISMS is required. Section 4.4 consolidates this gap together with those identified in Sections 4.1 and 4.2 into a unified set of supplementary measures.

4.4 Identified Gaps and Supplementary Measures

The preceding sections have systematically mapped the three focal areas of the NIS2 Directive - risk management (Article 21), incident reporting (Article 23), and supply chain security (Articles 21(2)(d) and 21(3)) - against the controls of ISO/IEC 27001:2022. The analysis reveals that while ISO 27001 provides a strong and largely compatible foundation, several specific gaps remain where the standard either lacks binding requirements or prescribes less granular measures than the directive demands. This section consolidates all identified gaps and proposes actionable supplementary measures that international companies operating in Finland can implement to achieve full NIS2 compliance without abandoning their existing

Information Security Management System (ISMS).

The gaps fall into four categories: (i) incident reporting timelines and external notification formats; (ii) multi-factor authentication prescriptiveness; (iii) individual supplier vulnerability assessment granularity; and (iv) management liability (a regulatory gap not addressed by ISO 27001). Each gap is presented below with a corresponding supplementary measure.

4.4.1 Gap: Binding Incident Reporting Timelines and External Notifications

Origin: Section 4.2 (Article 23(4)(a), (b), (c) and 23(2)).

Nature: ISO 27001 controls (A.5.24-A.5.26) establish an internal incident management process but contain no binding deadlines. The standard's "as quickly as possible" is not equivalent to NIS2's 24-hour early warning, 72-hour detailed notification, or one-month final report [3], [6]. Moreover, ISO 27001 does not mandate external reporting to a CSIRT or the notification of affected service recipients.

Supplementary measures:

1. **S1 - Adopt a NIS2 incident reporting procedure.** Create a documented process that is separate from, but linked to, the existing ISO 27001 incident management workflow. This procedure must specify:

    - A 24-hour early warning template that includes: incident date and time, nature of the incident, suspected malicious act (yes/no), and potential cross-border impact.
    - A 72-hour detailed notification template that includes: severity assessment (based on NIS2's €500,000 threshold or 5% global turnover), operational disruption level, initial impact analysis, and any known indicators of compromise (IoCs).

- A one-month final report template that includes: root cause analysis, applied and planned mitigation measures, cross-border implications, and lessons learned.
- Designation of a responsible person (e.g., CISO or Data Protection Officer) authorised to submit notifications to the competent authority or CSIRT within the prescribed timelines.
- A customer/recipient notification template to be used when a significant cyber threat affects service recipients (Article 23(2)).

2. **S2 - Integrate timeline tracking into the ISMS.** Modify the incident response log or use a dedicated ticketing system to record the exact time of awareness and track the 24-hour, 72-hour, and one-month deadlines. Include automated reminders and escalation procedures for missed deadlines.

4.4.2 Gap: Multi-Factor Authentication Prescriptiveness

Origin: Section 4.1 (Article 21(2)(j)).

Nature: ISO 27001 controls A.5.17 and A.8.5 require secure authentication but allow discretion ("where appropriate"). NIS2 expects MFA as a default for remote access, administrative access, and access to sensitive systems [3].

Supplementary measure:

1. **S3 - Implement a mandatory MFA policy that removes discretion.** Amend the organisation's access control policy to state: "Multi-factor authentication shall be required for all remote access to the corporate network, for all administrative accounts, and for access to any system or application handling personal data, operational technology, or critical business data." Exceptions (if any) must be justified in writing and approved by the CISO or a designated security committee. This policy should be referenced in the Statement

of Applicability (SoA) as a supplement to ISO 27001 A.5.17.

4.4.3 Gap: Individual Supplier Vulnerability Assessment Granularity

Origin: Section 4.3 (Article 21(3)).

Nature: ISO 27001 controls A.5.19-A.5.21 require supplier risk assessments but do not explicitly mandate an individual vulnerability assessment for each direct supplier. NIS2's phrasing ("vulnerabilities specific to each direct supplier") implies a more granular, per-supplier analysis [3], [6].

Supplementary measures:

1. **S4 - Enhance supplier assessment templates to per-supplier granularity.** Modify the existing supplier management process to require, for every direct supplier (including cloud service providers, software vendors, and managed service providers):

    - A documented identification of supplier-specific vulnerabilities (e.g., known CVEs affecting their products, weak security controls, sub-supplier dependencies).
    - An evaluation of the supplier's product quality (e.g., availability of security patches, incident history).
    - A review of the supplier's secure development procedures (e.g., compliance with ISO 27001, SOC 2, or equivalent standards).
    - A risk rating for the supplier based on the above granular analysis.
    - For critical suppliers (e.g., those with access to sensitive data or operational systems), reassessment at least annually and upon any significant change (e.g., acquisition, major software release).

2. **S5 - Maintain a supplier vulnerability register.** Create a central register that lists all direct suppliers, the identified vulnerabilities specific to each, and the status of mitigation (e.g., accepted, transferred, remediated by supplier). This register serves as auditable evidence for NIS2 compliance and is not required by ISO 27001 alone.

4.4.4 Gap: Management Liability

Origin: Not explicitly covered in the mapping tables, but referenced in the summary of gaps (Appendix A).

Nature: ISO 27001 Clause 5 (Leadership) requires top management to demonstrate leadership and commitment, but it does not impose personal legal liability for non-compliance. NIS2 Article 20 explicitly states that management bodies "shall be held liable for infringements" and must approve the cybersecurity risk-management measures [3].

Supplementary measure:

1. **S6 - Formalise management accountability in governance documents.**

   - Amend the board or management committee's terms of reference to explicitly state that responsibility for NIS2 compliance rests with a designated legal representative (e.g., CEO or managing director).
   - Document formal approval (e.g., board resolution or signed policy) of the NIS2-related risk management measures and incident reporting procedure.
   - Include a standing agenda item on NIS2 compliance status at every management review meeting (as required by ISO 27001 Clause 9.3).
   - Retain meeting minutes and approval records as evidence that management has been actively involved and can demonstrate due diligence.

4.4.5 Summary of Supplementary Measures

Table 4.1 consolidates the six supplementary measures and their alignment with the identified gaps. This table replaces the multiple figures previously used, providing a clear and concise overview of all gaps, their NIS2 references, corresponding supplementary measures, and implementation effort.

Table 4.1: Summary of identified gaps and corresponding supplementary measures

Gap Category	**NIS2 Reference**	**Supplementary Measure**	**Implementation Effort**
Incident reporting timelines & external notifications	Art. 23(4)(a),(b),(c); 23(2)	S1: NIS2 incident reporting procedure (templates, responsible person, customer notification)	Medium
Timeline tracking	Art. 23(4)	S2: Integrate deadline tracking into ISMS (ticketing system, reminders)	Low
Multi-factor authentication	Art. 21(2)(j)	S3: Mandatory MFA policy (no "where appropriate" discretion)	Low
Individual supplier vulnerability assessment	Art. 21(3)	S4: Per-supplier granular assessment templates; S5: Supplier vulnerability register	Medium
Management liability	Art. 20	S6: Formal governance documentation (board approval, meeting minutes)	Low

All supplementary measures are designed to be layered onto an existing ISO 27001-certified ISMS without requiring re-certification or major structural changes. Organisations should prioritise the incident reporting measures (S1 and S2) because non-compliance with timelines carries immediate financial penalties. The remaining measures can be implemented within standard ISMS continuous improvement cycles.

5 Discussion

This chapter interprets the findings presented in Chapter 4, synthesising the control-by-control mapping analysis into a coherent discussion of how international companies operating in Finland can leverage ISO/IEC 27001:2022 to achieve NIS2 compliance. The discussion is structured around three main sections. First, Section 5.1 develops an integrated implementation model that translates the identified gaps and supplementary measures into a practical, step-wise roadmap for organisations. Second, Section 5.2 examines the practical implications for international companies operating in the Finnish context, addressing sector-specific considerations, resource constraints, and the broader regulatory environment. Third, Section 5.3 reflects on the limitations of the study, distinguishing these from the methodological limitations already discussed in Chapter 3 by focusing on the applicability, generalisability, and interpretational constraints of the findings.

5.1 Towards an Integrated NIS2-ISO 27001 Implementation Model

The analysis in Chapter 4 demonstrated that ISO/IEC 27001:2022 provides a robust foundation for NIS2 compliance, with approximately 63.6% of the risk management requirements under Article 21 fully aligned with existing ISO controls [3], [6]. However, the remaining gaps - particularly in incident reporting timelines, multi-factor authentication prescriptiveness, individual supplier vulnerability assessment granularity, and management liability - require targeted supplementary measures that extend beyond the standard's

scope. Building on these findings, this section outlines an integrated implementation model that organisations can follow to systematically extend their existing ISMS for full NIS2 compliance.

The proposed model follows a phased, risk-prioritised approach that reflects the iterative nature of both ISO 27001's Plan-Do-Check-Act (PDCA) cycle and the NIS2 Directive's emphasis on ongoing risk management and continuous improvement [3], [6].

5.1.1 Phase 1: Gap Assessment and Prioritisation

Organisations should begin by conducting a systematic gap assessment using the mapping tables presented in Appendix A. This involves reviewing each NIS2 provision against existing ISO 27001 controls and documenting whether each requirement is fully satisfied, partially covered, or completely gapped. Table 4.1 (presented in Section 4.4) provides a consolidated summary of the identified gaps and their corresponding supplementary measures, serving as a practical starting point. Based on the gap assessment, remediation efforts should be prioritised according to risk exposure and regulatory urgency. Incident reporting measures (S1 and S2) should be accorded the highest priority, as non-compliance with the 24-hour, 72-hour, and one-month reporting timelines carries immediate financial penalties, with fines reaching up to €10 million or 2% of global annual turnover for essential entities [3]. Multi-factor authentication (S3) and supplier vulnerability assessment (S4 and S5) should follow, as these address high-impact security risks that are explicitly mandated by NIS2. Management liability (S6), while important for governance and accountability, can be addressed through documentation and procedural changes without significant technical investment.

5.1.2 Phase 2: Supplementary Measure Implementation

The second phase involves implementing the supplementary measures identified in Section 4.4. For incident reporting (S1 and S2), organisations must establish a dedicated NIS2 incident notification procedure that operates in parallel with the existing ISO 27001

incident management workflow. This procedure should include standardised templates for the three mandated reports (24-hour early warning, 72-hour detailed notification, and one-month final report), clear designation of responsible personnel, and integration of timeline tracking mechanisms. The procedure must also address customer and recipient notifications as required by Article 23(2) [3]. For multi-factor authentication (S3), organisations should amend their access control policy to mandate MFA by default for all remote access, administrative accounts, and systems handling sensitive data, removing the discretion permitted by ISO 27001 controls A.5.17 and A.8.5 [6]. For supplier vulnerability assessment (S4 and S5), organisations should enhance existing supplier management templates to include per-supplier vulnerability assessments, documenting supplier-specific vulnerabilities, evaluating product quality and secure development procedures, and assigning risk ratings based on a granular analysis. A central supplier vulnerability register should be maintained to provide auditable evidence. For management liability (S6), organisations should formalise accountability through governance documentation, including board resolutions, policy approvals, and standing agenda items on NIS2 compliance at management review meetings.

5.1.3 Phase 3: Integration, Documentation, and Continuous Improvement

The third phase focuses on integrating the supplementary measures into the organisation's existing ISMS documentation and governance structures. The Statement of Applicability (SoA) should be revised to include the supplementary measures as additional controls, with clear justifications. The risk treatment plan and incident response plan should be updated accordingly. All documentation should be version-controlled and stored in the research log described in Section 3.2.6, ensuring traceability and audit readiness. Organisations should conduct regular reviews of their NIS2 compliance status, incorporating lessons learned from incidents, audits, and regulatory updates, and internal audits should include specific checks for NIS2-related controls.

5.2 Practical Implications for International Companies in Finland

The findings of this thesis carry significant practical implications for international companies operating in Finland that are subject to the NIS2 Directive.

5.2.1 Strategic Opportunity: Leveraging Existing ISMS Investments

The analysis demonstrates that international companies with existing ISO 27001-certified ISMS are already well positioned to achieve NIS2 compliance. The full alignment of approximately 63.6% of NIS2 Article 21 requirements means that organisations can avoid substantial investment in building a compliance programme from scratch. For many large firms in manufacturing, digital infrastructure, and energy sectors that already maintain ISO 27001 certification, the incremental effort required to address the identified gaps is substantially lower than the cost of developing an entirely new compliance programme. The supplementary measures proposed in Section 4.4 are designed to be layered onto existing ISMS without requiring major structural changes or re-certification.

5.2.2 Operational Challenges: Resource Constraints and Regulatory Complexity

Despite this strategic opportunity, organisations face significant operational challenges. The most immediate challenge is the resource burden associated with documentation and procedural changes. Even where existing security practices are already strong, the supplementary measures - particularly incident reporting (S1 and S2) and supplier vulnerability assessment (S4 and S5) - require dedicated administrative effort. The NIS2 Directive acknowledges this through its principle of proportionality, requiring that measures be "appropriate and proportionate" to the entity's size, risk exposure, and sector [3]. The supplementary measures are designed to be scalable, with low-effort measures (S2, S3, S6)

prioritised for rapid implementation, and higher-effort measures (S1, S4 and S5) addressed through phased implementation plans. Additionally, the complexity of the regulatory landscape - with overlapping regulations such as GDPR, DORA, and the EU AI Act - requires organisations to maintain a single, extensible ISMS rather than separate compliance silos [8].

5.2.3 Sector-Specific Considerations: Finland's National Implementation

The Finnish national implementation of NIS2, as articulated in HE 57/2024 [7], introduces several sector-specific considerations. First, the proposal transposes the twelve risk management measure categories into binding national requirements, with supervisory authorities such as Traficom responsible for enforcement. Second, the Finnish National Cyber Security Centre (NCSC-FI) has developed the Kybermittari maturity assessment tool, which maps directly to the NIS2 risk management measures and provides a practical framework for self-assessment [36]. International companies can leverage Kybermittari to complement the ISO 27001-based mapping presented in this thesis. Third, Finland's high digital maturity and the presence of numerous international firms in critical infrastructure sectors mean that sector-specific variations may be significant. The implementation model is designed to be extensible, allowing organisations to incorporate sector-specific controls as needed.

5.2.4 Practical Recommendations

Based on the analysis, the following practical recommendations are offered: (1) conduct a systematic gap assessment using the mapping tables in Appendix A, prioritising incident reporting measures (S1 and S2); (2) update the ISMS Statement of Applicability to include the supplementary measures (S1-S6); (3) develop standardised incident reporting templates for the 24-hour, 72-hour, and one-month reports; (4) amend access control policies to mandate MFA by default; (5) enhance supplier management processes to include per-supplier vulnerability assessments and maintain a central supplier vulnerability regis-

ter; (6) formalise management accountability through governance documentation; and (7) leverage Finnish national tools such as Kybermittari to validate ISMS alignment.

5.3 Limitations of the Study

This section reflects on the limitations of the study, distinguishing these from the methodological limitations already discussed in Chapter 3. While Chapter 3 addressed limitations related to the research methodology - including the documentary-only approach, static mapping, and lack of empirical validation - this section focuses on the limitations of the applicability, generalisability, and interpretational constraints of the findings.

5.3.1 Interpretational Constraints

The mapping analysis involved a degree of interpretative judgement, particularly in classifying NIS2 requirements as "full alignment," "partial overlap," or "gap." While a systematic coding scheme was applied and documented by the student author, all mapping decisions, including certain principle-based provisions - such as "appropriate and proportionate measures" - were not considered in binary classification. Different practitioners might draw the boundary between "full" and "partial" differently. This thesis mitigates this by providing detailed justifications for each coding decision and proposing concrete supplementary measures.

5.3.2 Generalisability Constraints

The findings are based on the NIS2 Directive as transposed into Finnish national legislation via HE 57/2024 [7]. While the core mapping applies across all EU Member States, the Finnish national implementation introduces country-specific interpretations that may affect the applicability of the supplementary measures. Organisations operating in other Member States should adapt the model to their own national transposition. Additionally, the thesis focuses exclusively on ISO/IEC 27001:2022; other frameworks - such as NIST CSF, C2M2,

or sector-specific standards - may offer alternative pathways to compliance, and the findings are conditional on the organisation having or intending to adopt an ISO 27001-based ISMS.

5.3.3 Assumptions about Organisational Maturity and Temporal Constraints

The integrated implementation model assumes a baseline level of organisational maturity in information security management, specifically that organisations have already implemented an ISO 27001-certified ISMS. For organisations with less mature security programmes, the supplementary measures alone will be insufficient. The model also assumes that organisations have the resources and commitment to implement the measures; while they are designed to be scalable, smaller or resource-constrained organisations may struggle with administrative effort. The mapping analysis is static and tied to the 2022 versions of both the NIS2 Directive and ISO 27001. Future amendments - such as the Commission Implementing Regulation (EU) 2024/2690 - may affect the alignment, and the findings should be re-evaluated when official updates occur [12].

5.3.4 Lack of Empirical Validation

Finally, the proposed implementation model remains conceptual and has not been empirically validated through case studies or action research in actual international companies operating under NIS2 supervision in Finland. This thesis demonstrates that the mapping and supplementary measures are theoretically sound and grounded in established standards, but the practical feasibility and effectiveness have not been tested. Future research should validate the model through case studies or action research, examining implementation costs, practical obstacles, and unforeseen gaps that a purely document-based analysis cannot detect. Despite these limitations, the findings provide a robust foundation for international companies in Finland to navigate NIS2 compliance using their existing ISO 27001-based ISMS.

6 Conclusion and Recommendations

This final chapter concludes the thesis by summarising the key findings, offering actionable recommendations for practitioners, and suggesting directions for future research. The chapter is organised into three sections: Section 6.1 synthesises the main contributions of the study in relation to the research questions and objectives; Section 6.2 provides practical recommendations for international companies operating in Finland; and Section 6.3 identifies avenues for further investigation.

6.1 Summary of Key Findings

This thesis set out to examine how international companies operating in Finland can implement the NIS2 Directive through the ISO/IEC 27001:2022 framework. Two research questions guided the inquiry: **RQ1** (how ISO 27001 can be systematically mapped and utilised for NIS2 compliance) and **RQ2** (what are the strengths, limitations, and gaps of ISO 27001 for addressing NIS2 provisions on risk management, incident reporting, and supply chain security). These questions were addressed through three research objectives: **RO1** (mapping NIS2 requirements onto ISO 27001 controls), **RO2** (evaluating strengths and limitations), and **RO3** (identifying supplementary measures and proposing an implementation model).

The analysis in Chapter 4 demonstrated that ISO/IEC 27001:2022 provides a robust foundation for NIS2 compliance, with approximately 63.6% of Article 21 risk management requirements fully aligned with existing ISO controls [3], [6]. Seven provisions of Article 21 were classified as full alignments, including policies on risk analysis, supply chain security,

secure development, effectiveness assessment, cyber hygiene, cryptography, and human resources security. Four provisions were classified as partial overlaps requiring supplementary measures: incident handling (binding timelines), business continuity (crisis management), multi-factor authentication (prescriptiveness), and supplier vulnerability assessment (granularity). No provisions were completely uncovered.

For Article 23 on incident reporting, the findings revealed more significant gaps. ISO 27001 provides a sound internal incident management framework but lacks binding external reporting timelines. Three provisions were partially covered (definition of significant incidents, final reporting within one month, and notification of affected recipients), while two provisions were completely gapped (24-hour early warning and 72-hour detailed notification). These findings confirm that ISO 27001 alone is insufficient for meeting NIS2's prescriptive reporting obligations.

For supply chain security (Articles 21(2)(d) and 21(3)), ISO 27001 fully addresses the general obligation to manage supplier relationships but only partially covers the requirement for individual vulnerability assessments of each direct supplier. This granularity gap requires organisations to enhance their existing supplier management templates.

In response to these gaps, six supplementary measures (S1-S6) were proposed: (S1) a dedicated NIS2 incident reporting procedure with standardised templates; (S2) integration of timeline tracking into the ISMS; (S3) a mandatory MFA policy removing discretion; (S4) per-supplier granular assessment templates; (S5) a central supplier vulnerability register; and (S6) formalised management accountability through governance documentation. These measures are designed to be layered onto an existing ISO 27001-certified ISMS without requiring re-certification.

The thesis thus answers **RQ1** by demonstrating that ISO 27001 can be systematically mapped to NIS2 requirements through a control-by-control comparison, and **RQ2** by identifying specific strengths (full alignment of most risk management controls) and limitations (gaps in reporting timelines, MFA prescriptiveness, supplier granularity, and management liability). These contributions satisfy **RO1**, **RO2**, and **RO3** by providing a complete mapping, evaluating the framework's adequacy, and proposing a practical implementation

model.

6.2 Recommendations for Practitioners

Based on the findings, the following actionable recommendations are offered for international companies operating in Finland that are subject to the NIS2 Directive:

1. Conduct a systematic gap assessment using the mapping tables in Appendix A as a reference. Prioritise incident reporting measures (S1 and S2) as the highest priority due to regulatory deadlines and financial penalties, with fines reaching up to €10 million or 2% of global annual turnover for essential entities [3].

2. Update the ISMS Statement of Applicability (SoA) to include the supplementary measures (S1-S6) as additional controls, with clear justifications and traceability to NIS2 requirements. This ensures that the ISMS documentation remains comprehensive and audit-ready.

3. Develop and implement standardised incident reporting templates for the 24-hour early warning, 72-hour detailed notification, and one-month final report. Include timeline tracking mechanisms and designate responsible personnel for submission to the competent authority or CSIRT.

4. Amend access control policies to mandate MFA by default for all remote access, administrative accounts, and systems handling sensitive data. Remove the discretion permitted by ISO 27001 controls A.5.17 and A.8.5, and reference the revised policy in the SoA [6].

5. Enhance supplier management processes to include per-supplier vulnerability assessments. Maintain a central supplier vulnerability register listing identified vulnerabilities, product quality evaluations, secure development procedure reviews, and risk ratings. For critical suppliers, conduct reassessments at least annually.

6. Formalise management accountability through governance documentation. Designate a specific legal representative responsible for NIS2 compliance, document formal approval of NIS2-related policies, and establish a standing agenda item on NIS2 compliance status at management review meetings. Retain meeting minutes and approval records as evidence.

7. Leverage Finnish national tools such as Kybermittari to validate ISMS alignment with supervisory authority expectations and to support continuous improvement [36]. The Kybermittari maturity assessment tool maps directly to NIS2 risk management measures and provides a practical framework for self-assessment.

6.3 Future Research Directions

While this thesis has provided a systematic mapping and implementation model, several avenues for future research remain:

1. Empirical validation of the implementation model through case studies or action research in actual international companies operating under NIS2 supervision in Finland. Such research would examine implementation costs, practical obstacles, and unforeseen gaps that a purely document-based analysis cannot detect.

2. Comparative analysis of compliance frameworks across different sectors (e.g., manufacturing vs. energy vs. digital infrastructure) to identify sector-specific variations that may require tailored supplementary measures beyond the general model proposed here.

3. Future research should include longitudinal studies tracking the evolution of the Finnish national implementation now that the final legislation (the Cybersecurity Act) has been enacted. This would provide insights into how national-level interpretations affect the practical application of the supplementary measures proposed in this thesis.

4. Integration of other overlapping EU regulations such as GDPR, DORA, and the EU AI Act into the implementation model [8]. Future research could develop a unified compliance framework that addresses multiple regulatory obligations through a single, extensible ISMS.

5. Development of automated mapping tools that can dynamically update the alignment between NIS2 requirements and ISO 27001 controls as both instruments evolve. This would help organisations maintain compliance over time without repeating manual mapping exercises.

By pursuing these research directions, the academic and practical understanding of NIS2 implementation through ISO 27001 can be further advanced, supporting international companies in their journey towards effective cybersecurity governance and regulatory compliance.

References

[1] International Business Machines Corporation, "Cost of a data breach report 2025", Tech. Rep., 2025. [Online]. Available: https://www.ibm.com/reports/data-breach.

[2] European Union Agency for Cybersecurity (ENISA), "ENISA threat landscape 2025", Tech. Rep., 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[3] 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 (NIS2 directive)", *Official Journal of the European Union*, vol. L 333/80, Dec. 2022.

[4] European Commission, *NIS2 directive transposition in EU countries*, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-transposition.

[5] 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*, vol. L 194/1, 2016.

[6] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27001:2022 - information security, cybersecurity

and privacy protection - information security management systems - requirements", ISO/IEC, Geneva, Switzerland, Tech. Rep., 2022.

[7] Finnish Parliament, *Hallituksen esitys HE 57/2024 vp*, 2024. [Online]. Available: https://www.eduskunta.fi/valtiopaivaasiat/HE+57/2024.

[8] 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 (DORA)", *Official Journal of the European Union*, vol. L 333/1, 2022. [Online]. Available: http://data.europa.eu/eli/reg/2022/2554/oj.

[9] National Institute of Standards and Technology, "The NIST cybersecurity framework (CSF) 2.0", Tech. Rep., 2024. DOI: 10.6028/NIST.CSWP.29.

[10] European Commission, *NIS2 directive: Securing network and information systems*, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[11] NIS2 Resources, *Article 21, cybersecurity risk-management measures - NIS2 directive (EU) 2022/2555*, 2024. [Online]. Available: https://nis2resources.eu/directive-2022-2555-nis2/article-21/.

[12] European Union, "Commission implementing regulation (EU) 2024/2690 of 17 october 2024 laying down rules for the application of directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures", *Official Journal of the European Union*, vol. L series, Oct. 2024.

[13] 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.

[14] European Union Agency for Cybersecurity (ENISA), "NIS2 technical implementation guidance", Tech. Rep., 2025. [Online]. Available: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

[15] European Union Agency for Cybersecurity (ENISA), *Supporting NIS2 implementation through actionable guidance*, Jun. 2025. [Online]. Available: https://www.enisa.europa.eu/news/supporting-nis2-implementation-through-actionable-guidance.

[16] Certified Information Security, *A certified NIST cybersecurity framework 2.0 lead implementer (CSF LI)*. [Online]. Available: https://niccs.cisa.gov/training/catalog/cis/certified-nist-cybersecurity-framework-20-lead-implementer-csf-li.

[17] International Accreditation Forum (IAF), "IAF mandatory document for the transition requirements for ISO/IEC 27001:2022", International Accreditation Forum, Tech. Rep. IAF MD 26:2023, 2023. [Online]. Available: https://iaf.nu/iaf_system/uploads/documents/IAF_MD_26_Transition_requirements_for_ISOIEC_27001-2022_09082022.pdf.

[18] Cisco Systems, *Framework mapping: Cisco secure workload + NIS2 and ISO 27001:2022 solution guide*, Feb. 2026. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/secure-workload/nis2-iso-27001-sg.html.

[19] European Commission, "Mapping of cybersecurity standards to EU legislation", Publications Office of the European Union, Luxembourg, Tech. Rep., 2024. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC137340.

[20] European Union Agency for Cybersecurity (ENISA), "Standardisation in support of the cybersecurity certification", ENISA, Heraklion, Greece, Tech. Rep.,

2019. [Online]. Available: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i.

[21] European Union, "Regulation (EU) 2019/881 of the european parliament and of the council of 17 april 2019 on ENISA and on information and communications technology cybersecurity certification (cybersecurity act)", *Official Journal of the European Union*, vol. L 151/15, Jun. 2019.

[22] T. Mettler, "Maturity assessment models: A design science research approach", *International Journal of Society Systems Science*, vol. 3, no. 1/2, pp. 81–98, 2011.

[23] 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, 2024. DOI: 10.1016/j.accinf.2024.100695.

[24] 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, Tech. Rep., 2021. DOI: 10.2759/184749.

[25] K. Uutela, "Cybersecurity standards-based model for IT/OT converged environments", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, May 2025.

[26] A. van Welie, "Legislation within cybersecurity: Preparing for NIS2 - a detailed framework in the healthcare sector in the netherlands", M.S. thesis, Turku School of Economics, Univ. Turku, Turku, Finland, Jul. 2024.

[27] CMS Law-Now, *Decoding the NIS2 directive: Practical guidelines from the EU agency for cybersecurity on NIS2 risk management and skills*, Aug. 2025. [Online]. Available: https://cms-lawnow.com/en/ealerts/2025/08/decod

ing-the-nis2-directive-practical-guidelines-from-the-eu-agency-for-cybersecurity-on-nis2-risk-management-and-skills.

[28] National Cyber Security Centre Finland, *Kybermittari - aineistot - import-työkalu (3.2.2025)*, 2025. [Online]. Available: https://kyberturvallisuuskeskus.fi/fi/saadokset/suositus-nis-valvoville-viranomaisille-kyberturvallisuuden-riskienhallinnan-toimenpiteista.

[29] A. Bowo, "Adapting cybersecurity frameworks for NIS2 compliance", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, Apr. 2025.

[30] K. Fransila, "Implementing NIS2 EU directive to large international company in finland", M.S. thesis, Metropolia Univ. Appl. Sci., Helsinki, Finland, Mar. 2024.

[31] A. Trent, "Compliance analysis for cyber security marine standards", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, Jun. 2023.

[32] M. Suksi, "Software development compliance: Translating EU cybersecurity legislation into practice for IoT and embedded systems", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, Oct. 2025.

[33] J. W. Creswell and C. N. Poth, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, 4th. Thousand Oaks, CA, USA: SAGE Publications, 2018.

[34] K. Krippendorff, *Content Analysis: An Introduction to Its Methodology*, 4th. Thousand Oaks, CA, USA: SAGE Publications, 2018.

[35] R. K. Yin, *Case Study Research and Applications: Design and Methods*, 6th. Thousand Oaks, CA, USA: SAGE Publications, 2018.

[36] Finnish Transport and Communications Agency (Traficom), "LUONNOS suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä", Tech. Rep. Traficom/18410/09.00.02/2023, 2024.

[37] V. Mlačić, "Data protection regulation ontology for compliance", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, Jun. 2022.

[38] K. Vahteri, "Framework for SOC performance metrics and enhancement", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, Oct. 2025.

[39] K. Papaleonidas, "Classified information in cloud services - new era of cyber security", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, Jun. 2025.

[40] Y. Wang, "A comparative study of chinese and european internet companies' privacy policy based on knowledge graph", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, Jun. 2019.

[41] J. Reilimo, "Preparedness against cybersecurity threats - a study of SMEs in the nordic region", M.S. thesis, Turku School of Economics, Univ. Turku, Turku, Finland, Nov. 2020.

[42] E. Tynys, "The effects of recent EU regulations on software development", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, May 2025.

[43] J. E. Opuda, "Implementation of ISO frameworks to risk management in IPv6 security", M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, May 2023.

[44] European Union Agency for Cybersecurity (ENISA), "ENISA threat landscape 2024", Tech. Rep., 2024. [Online]. Available: `https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024`.

[45] NIS2 Resources, *Article 23, reporting obligations - NIS2 directive (EU) 2022/2555*, 2024. [Online]. Available: `https://nis2resources.eu/directive-2022-2555-nis2/article-23/`.

[46] European Union Agency for Cybersecurity (ENISA), "ENISA threat landscape 2023", Tech. Rep., 2023. [Online]. Available: `https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023`.

[47] NIS Cooperation Group, "Reference document on incident notification for operators of essential services. circumstances of notification", Tech. Rep. 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.

[48] National Cyber Security Centre, *NCSC: NIS2 essential and important entities*, 2023. [Online]. Available: https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_2_ENTITIES.pdf.

[49] U.S. Department of Energy, *Cybersecurity capability maturity model (C2M2)*, 2025. [Online]. Available: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

[50] U.S. Department of Energy, *About the cybersecurity capability maturity model (C2M2)*, 2025. [Online]. Available: https://c2m2.doe.gov/about.

[51] European Union Agency for Cybersecurity, *National cybersecurity assessment framework (NCAF) tool*, 2025. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncaf.

[52] European Union Agency for Cybersecurity, *CSIRT maturity framework*, 2025. [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity.

[53] International Organization for Standardization and International Electrotechnical Commission, "ISO/IEC 27004:2016 - information technology - security techniques - information security management - monitoring, measurement, analysis and evaluation", ISO/IEC, Geneva, Switzerland, Tech. Rep., 2016.

[54] International Business Machines Corporation, "IBM security x-force threat intelligence index 2024", Tech. Rep., 2024. [Online]. Available: https://www.ibm.com/reports/threat-intelligence.

[55] World Economic Forum, "Global risks report 2024", Tech. Rep., 2024. [Online]. Available: https://www.weforum.org/publications/global-risks-report-2024/digest/.

[56] D. Weston, *Helping our customers through the crowdstrike outage*, The Official Microsoft Blog, Jul. 2024. [Online]. Available: https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

[57] International Telecommunication Union, "Global cybersecurity index", Tech. Rep., 2024. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

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

[59] 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.

[60] 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.

[61] Cybersecurity and Infrastructure Security Agency, "APT cyber tools targeting ICS/SCADA devices", Tech. Rep., 2022. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-103a.

[62] Dragos Inc., *CHERNOVITE threat activity group*. [Online]. Available: https://www.dragos.com/threat/chernovite/.

[63] European Union Agency for Cybersecurity, *Cybersecurity policies*. [Online]. Available: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies.

[64] 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.

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

[66] Center for Internet Security, "CIS critical security controls, version 8.1", Tech. Rep., 2024. [Online]. Available: https://www.cisecurity.org/controls/.

[67] Cybersecurity and Infrastructure Security Agency, "Zero trust maturity model, version 2.0", Tech. Rep., 2023. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model.

[68] Microsoft Corporation, *Announcing the microsoft sentinel: Cybersecurity maturity model certification (CMMC) 2.0 solution*, Microsoft Sentinel Blog. [Online]. Available: https://techcommunity.microsoft.com/blog/microsoftsentinelblog/announcing-the-microsoft-sentinel-cybersecurity-maturity-model-certification-cmm/3295095.

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

[70] K. Dempsey et al., "Information security continuous monitoring (ISCM) for federal information systems and organizations", NIST, Tech. Rep. Special Publication (SP) 800-137, 2011. DOI: 10.6028/NIST.SP.800-137.

Appendix A NIS2–ISO 27001:2022 Control Mapping Matrix

Table A.1 – Risk Management Requirements (NIS2 Article 21)

Table A.1: Risk Management Requirements – NIS2 Art. 21 mapped to ISO/IEC 27001:2022

NIS2 Requirement (Art. 21)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
21(2)(a) Policies on risk analysis and information system security	A.5.1 (Policies for information security); A.5.8 (Information security in project management); Clause 6.1 (Actions to address risks)	F	ISO 27001 mandates documented security policies approved by management and a formal risk assessment process, fully covering the requirement.

Continued on next page

Table A.1 – continued from previous page

NIS2 Requirement (Art. 21)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
21(2)(b) Incident handling	A.5.24 (Incident management planning); A.5.25 (Assessment and decision on events); A.5.26 (Response to incidents)	P	Controls cover preparation, classification, and response, but ISO 27001 does not prescribe binding timelines (e.g., 24-hour early warning). Supplementary procedure needed for NIS2 timeline compliance.
21(2)(c) Business continuity, backup, disaster recovery, crisis management	A.5.29 (Information security during disruptions); A.5.30 (ICT readiness for business continuity)	P	The 2022 revision added control A.5.30, which aligns well with continuity requirements. However, NIS2 explicitly includes "crisis management" – ISO 27001 covers this indirectly under A.5.29, but may need reinforcement.

Continued on next page

Table A.1 – continued from previous page

NIS2 Requirement (Art. 21)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
21(2)(d) Supply chain security	A.5.19 (Supplier relationships); A.5.20 (Supplier agreements); A.5.21 (ICT supply chain management)	F	The three supplier-related controls collectively address identification, contractual security, and ICT supply chain risks, matching NIS2's requirements for direct suppliers.
21(2)(e) Security in acquisition, development, maintenance and vulnerability handling	A.5.14 (Secure development); A.5.8 (Project management); A.8.25 (Secure development life cycle); A.8.8 (Management of technical vulnerabilities)	F	Multiple controls cover the entire lifecycle. Vulnerability handling (A.8.8) explicitly includes disclosure processes.
21(2)(f) Policies to assess effectiveness of cybersecurity risk-management measures	Clause 9.1 (Monitoring, measurement, analysis, evaluation); Clause 9.2 (Internal audit); Clause 9.3 (Management review)	F	The Plan-Do-Check-Act (PDCA) cycle requires regular effectiveness assessment, internal audits, and management reviews – fully aligned.

Continued on next page

Table A.1 – continued from previous page

NIS2 Requirement (Art. 21)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
21(2)(g) Basic cyber hygiene and cybersecurity training	A.6.3 (Information security awareness, education, training); A.5.36 (Compliance with policies)	F	ISO 27001 requires ongoing awareness programmes and verification of adherence to policies, covering hygiene and training.
21(2)(h) Policies on cryptography and encryption	A.5.31 (Legal, statutory, regulatory and contractual requirements – encryption aspects); A.8.24 (Use of cryptography)	F	Controls mandate a documented cryptographic policy, key management, and appropriate use of encryption.
21(2)(i) Human resources security, access control, asset management	A.5.9 (Asset inventory); A.5.15 (Access control); A.5.16 (Identity management); A.5.17 (Authentication information); A.5.18 (Access rights); Clause 6 (People controls – A.6.1 to A.6.8)	F	Comprehensive coverage of asset management, access governance, and human-centric security measures (screening, responsibilities, disciplinary process).

Continued on next page

Table A.1 – continued from previous page

NIS2 Requirement (Art. 21)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
21(2)(j) Multi-factor authentication or continuous authentication	A.5.17 (Authentication information); A.8.5 (Secure authentication)	P	ISO 27001 requires secure authentication but does not mandate MFA as a default. The standard states "where appropriate", leaving discretion. NIS2 is more prescriptive. Supplementary MFA policy needed.
21(3) Supply chain vulnerability assessment (each direct supplier)	A.5.19 to A.5.21 (as above) plus Clause 8.1 (Operational planning – external providers)	P	ISO 27001 addresses supplier risk assessment but does not explicitly require *individual* vulnerability assessment for *each* direct supplier at the level of detail implied by NIS2. A more granular procedure may be needed.

Table A.2 – Incident Reporting Requirements (NIS2 Article 23)

Table A.2: Incident Reporting Requirements – NIS2 Art. 23 mapped to ISO/IEC 27001:2022

NIS2 Requirement (Art. 23)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
23(3) Definition of "significant incident" (severe operational disruption, financial loss, material damage)	A.5.25 (Assessment and decision on events)	P	ISO 27001 requires classification of events as incidents but does not prescribe the quantitative thresholds (e.g., financial loss > €500k) or qualitative criteria of NIS2. Organisation must adopt NIS2 criteria into its classification scheme.
23(4)(a) Early warning within 24 hours (including malicious act suspicion and cross-border impact)	A.5.25 (Assessment) and A.5.26 (Response) – but no timeline	G	ISO 27001 contains no binding timeline for initial notification. "As quickly as possible" is not equivalent to 24 hours. Dedicated early-warning procedure required.

Continued on next page

Table A.2 – continued from previous page

NIS2 Requirement (Art. 23)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
23(4)(b) Incident notification within 72 hours (severity, impact, IOCs)	None	G	ISO 27001 does not specify a 72-hour detailed notification to an external authority. The standard's communication clauses (Clause 7.4) are generic.
23(4)(c) Final report within one month (root cause, mitigation, cross-border impact)	A.5.26 (Response) and Clause 10.1 (Nonconformity and corrective action)	P	ISO 27001 requires root cause analysis and corrective actions, but it does not mandate a final report to an external CSIRT or within a one-month deadline. The content (root cause, mitigation) is covered; the external reporting format and timeline are gaps.

Continued on next page

Table A.2 – continued from previous page

NIS2 Requirement (Art. 23)	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
23(2) Notify affected service recipients of significant cyber threats and remediation measures	A.7.4 (Communication with specific interest groups)	P	ISO 27001 provides a framework for external communication but does not specifically require notifying recipients of a cyber threat or prescribing the content of such notification. Additional procedure needed.

Table A.3 – Supply Chain Security (Detailed from Art. 21(2)(d) and Art. 21(3))

Table A.3: Supply Chain Security – Detailed NIS2 Requirements mapped to ISO/IEC 27001:2022

NIS2 Requirement	**ISO/IEC 27001:2022 Control(s)**	**Alignment**	**Justification**
21(2)(d) Address security-related aspects concerning relationships with direct suppliers or service providers	A.5.19 (Supplier relationships); A.5.20 (Supplier agreements); A.5.21 (ICT supply chain management)	F	The three controls together require risk assessment, contractual security clauses, monitoring, and supply chain-specific risk management, fully aligning with the provision.
21(3) Consider vulnerabilities specific to each direct supplier and the overall quality of products and cybersecurity practices, including secure development procedures	A.5.21 (ICT supply chain management) plus A.5.19 (risk assessment)	P	ISO 27001 covers product quality and secure development expectations in supplier agreements but does not explicitly mandate *individual* vulnerability assessment for *each* direct supplier. The phrase "each direct supplier" implies a more granular level of analysis than the standard's typical "risk-based" approach. Organisations may need to enhance their supplier assessment templates.

Summary of Gaps Requiring Supplementary Measures

- **Incident reporting timelines** - ISO 27001 lacks the 24-hour early warning, 72-hour detailed notification, and one-month final report deadlines. A dedicated NIS2 incident notification procedure must be added to the ISMS.
- **Multi-factor authentication** - ISO 27001 allows discretion ("where appropriate"), whereas NIS2 expects MFA as a default for remote access and sensitive systems. A stricter MFA policy should be embedded.
- **Individual supplier vulnerability assessment** - The level of granularity required by NIS2 Art. 21(3) (each direct supplier) may exceed the standard's risk-based sampling. Consider a formalised supplier-by-supplier assessment template.
- **Management liability** - ISO 27001 requires top management commitment (Clause 5) but does not impose personal legal liability. This is a regulatory, not a technical, gap; it must be addressed through governance documentation and board-level accountability statements.

How to read this matrix: The classification "F" (full alignment) indicates that implementing the ISO control as written will satisfy the corresponding NIS2 requirement without modification. "P" (partial overlap) means the ISO control provides a foundation but must be supplemented by an organisational procedure to fully meet the NIS2 obligation. "G" (gap) means ISO 27001 provides no relevant control, and a completely new measure must be implemented. The justifications column explains each decision and directs the reader to the supplementary measures proposed in Chapter 5.5.

Note on version control: This mapping is based on NIS2 Directive (EU 2022/2555) as published in December 2022 and ISO/IEC 27001:2022. Future amendments to either instrument may require revision of this matrix. The methodological steps described in Section 3.2 remain applicable for updating the mapping.