Linda Turtola

Evaluating the Impact of the Revised Network and Information Security Directive on supply chain and supplier relationship risk management of Electricity Distribution System Operators

Tekniikan ja innovaatiojohtamisen yksikkö
Master’s Thesis in Industrial Management
Master's Programme in Industrial Management

Vaasa 2024

UNIVERSITY OF VAASA
Tekniikan ja innovaatiojohtamisen yksikkö
Author: Linda Turtola
Title of the thesis: Evaluating the Impact of the Revised Network and Information Security Directive on supply chain and supplier relationship risk management of Electricity Distribution System Operators [Subject]
Degree: Master of Science in Economics and Business Administration
Discipline: Master's Programme in Industrial Management
Supervisor: Petri Helo
Year: 2024 **Pages:** 96

ABSTRACT:

Energy sector is one of the essential components of the critical infrastructure. Cyberattacks can pose catastrophic consequences for society. Cyber-attacks targeting the supply chain have been recognized as one major vulnerability factor, prompting European Union to revise the Network and Information Security directive (NIS2). The management of supply chain cybersecurity risks is now integrated to NIS2 risk management measures.

This thesis considers the existing state of the operational landscape of the electricity distribution system operators (DSOs) as well as the cybersecurity risk management measures utilized in the supply chains. The different methods for cybersecurity management are explored through two thematic levels which are supplier risk management and product risk management. The thesis aims to create a guideline for electricity distribution system operators (DSO) for the revised network and information security directive (NIS2) compliance by highlighting the special cybersecurity features in their supply chains.

This work focuses on analysing upcoming cybersecurity regulations from the perspective of electricity distribution operators. The research method is design science. The thesis is a case study case study focusing on two separate DSOs. The thesis provides a litetarure review on the topic. Data is gathered with interviews and surveys from the two DSOs and external experts. The results are collated and analysed with the aim of providing applicable recommendations.

The recommendations given are that the DSO's should assess the risks of managing the cybersecurity at the group company level. Secondly, they should ensure unified agreement of how the supplier and service provider list is done. DSO's should enhance the cybersecurity practices integrated to risk assessment frameworks and tailor the frameworks suitable for assessing individual suppliers. DSO's should also consider what frameworks their suppliers already use. The process for setting and documenting the requirements for cybersecurity in contracts should be unified. Additionally, a special focus should be on the component level cyber security when procuring products that have software. If and when possible, these activities should be performed in cooperation with internal and external stakeholders to maintain the high security level of complete sector.

KEYWORDS: the Revised Network and Information Security Directive, cybersecurity, supply chain risk management.

VAASAN YLIOPISTO
Tekniikan ja innovaatiojohtamisen yksikkö
Tekijä: Linda Turtola
Tutkielman nimi: Evaluating the Impact of the Revised Network and Information Security Directive on supply chain and supplier relationship risk management of Electricity Distribution System Operators [Subject]
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Tuotantotalouden maisteriohjelma
Työn ohjaaja: Petri Helo
Valmistumisvuosi: 2024 **Sivumäärä:** **96**

TIIVISTELMÄ:
Energia-ala on yksi kriittisen infrastruktuurin olennaisista osista. Kyberhyökkäykset voivat aiheuttaa katastrofaalisia seurauksia yhteiskunnalle. Toimitusketjuun kohdistuvat kyberhyökkäykset on tunnustettu yhdeksi suureksi haavoittuvuustekijäksi. Osittain tästä syystä Euroopan unioni on päättänyt uudistaa sen verkko- ja tietoturvadirektiiviä. Toimitusketjun kyberturvallisuusriskien hallinta on nyt integroitu uudistetun direktiivin riskienhallintatoimenpiteisiin.

Tässä pro gradu -tutkielmassa tarkastellaan sähkönjakeluverkkoyhtiöiden toimintaympäristön nykytilaa sekä toimitusketjuissa hyödynnettäviä kyberturvallisuusriskien hallintatoimenpiteitä. Kyberturvallisuuden hallinnan eri menetelmiä tarkastellaan kahdella eri temaattisella tasolla, jotka ovat toimittajariskien hallinta ja tuoteriskien hallinta. Tutkielman tavoitteena on luoda sähkönjakeluverkkoyhtiöille ohjeistus uudistetun verkko- ja tietoturvadirektiivin noudattamiselle samalla ottaen huomioon heidän toimitusketjujensa kyberturvallisuuden erityispiirteitä.

Tämä työ keskittyy tulevien kyberturvallisuusmääräysten analysointiin sähkönjakeluyritysten näkökulmasta. Tutkielma tehdään suunnittelutieteen menetelmällä. Tutkielma on tapaustutkimus, joka keskittyy kahteen erilliseen verkonhaltijaan. Tutkielma sisältää kirjallisuuskatsauksen, joka syventyy tutkielman aihepiiriin. Data kerätään kahden sähkönjakeluverkkoyhtiön ja ulkopuolisten asiantuntijoiden haastatteluilla ja tutkimuksilla. Tulokset kootaan ja analysoidaan soveltuvien suositusten antamiseksi.

Annetut suositukset ovat, että jakeluverkkoyhtiöiden tulisi arvioida kyberturvallisuuden hallinnan riskejä konserniyhtiötasolla. Toiseksi niiden tulisi varmistaa yhtenäinen näkemys siitä, miten tavarantoimittaja- ja palveluntarjoajaluettelo tehdään. Jakeluverkkoyhtiöiden tulisi tehostaa riskinarviointimalleihin integroituja kyberturvallisuuskäytäntöjä ja räätälöidä yksittäisten toimittajien arviointiin soveltuvat viitekehykset. Jakeluverkkoyhtiöiden tulisi myös harkita, mitä kyberturvallisuuden hallinnan malleja heidän toimittajansa jo käyttävät. Myös sopimusten kyberturvallisuusvaatimusten asettamis- ja dokumentointiprosessi tulee yhtenäistää. Lisäksi komponenttitason kyberturvallisuuteen tulisi kiinnittää erityistä huomiota hankittaessa tuotteita, joissa on ohjelmistoa. Nämä toimet tulisi mahdollisuuksien mukaan toteuttaa yhteistyössä sisäisten ja ulkoisten sidosryhmien kanssa koko alan korkean turvallisuustason ylläpitämiseksi.

AVAINSANAT: the Revised Network and Information Security Directive, cybersecurity, supply chain risk management.

Contents

Figures

Tables

Abbreviations

EU European Union
DSO Distribution System Operator
NIS Network and Information Security Directive (EU) 2016/1148

NIS Network and Information System
NIS2 The Revised Network and Information Security Directive (EU) 2022/2555
CER Directive on the resilience of critical entities Directive (EU) 2022/2557
CI Critical infrastructure
IT Information technology
OT Operational technology
SCADA Supervisory Control and Data Acquisition
DMS Distribution Management Systems
CRM Customer Relationship Management
ERP Enterprise Resource Management
EMS Energy Management System
AMI Advanced Metering Infrastructure
SCM Supply chain management

1 Introduction

The European Union (EU) is introducing new cybersecurity legislation during the year 2024, such as a revised version of the Network and Information Security Directive (NIS2), justified by the need of evolved cybersecurity measures for protecting the EU internal market. The EU Commission (2024a) has stated that the need for enhancing the cybersecurity measures has expanded after the COVID-19 pandemic and the digital leap of industry that happened as a result. Digitalization has resulted in organizations and systems becoming more interconnected. Due to the increased interconnectedness of the different operators of the society, any cybersecurity incident targeted towards a single entity can result to cascading effects. EU considers particularly concerning if a cyber attack is targeted towards the critical infrastructure (CI). CI is defined by Smith and Wilsons (2023) as the systems, assets and services necessary for society to function. Along with the NIS2 Directive EU has introduced another directive. This is the Directive on the resilience of critical entities (CER Directive), that establishes a framework through which entities of critical infrastructure can be identified. Organizations classified as critical infrastructure, such as energy sector and its subsectors, are subject to particularly strict compliance requirements. As such, the compliance with NIS2 requirements is mandated by them. These organizations have to incorporate the legislative cybersecurity requirements into their operations. These requirements include risk management measures, such as supply chain cyber risk management. (Directive (EU) 2022/2555; Directive (EU) 2022/2557; Smith & Wilsons, 2023; European Commission, 2024a; European Commission, 2023)

The supply chain aspect of NIS2 is described for instance in the recital (85) and article 22 part (d) and (e) of the directive. The article requires entities within its the scope to establish risk management procedures for their supply chains. These procedures involve for example assessing the cyber risk of their supply chain partners as well as integrating risk management requirements into contracts when for instance procuring a product or a service. The implementation of the legislation has been estimated to entail costs for the companies required to comply with NIS2, although there are also arguments on the

behalf of the directive. For instance, Finnish Information Security Cluster (FISC) claims (2024) that by complying with NIS2 directive, organizations enhance the societal cyber resilience and simultaneously increase their competitive advantage. This is rationalized by a claim that the faster the requirements of the law are achieved, the more likely the customer is to favour the supplier that thoroughly meets and demonstrates compliance. However, it has also been recognized by for instance that smaller companies have different premises for compliance compared to larger companies due to for example size of personnel and budget. (Directive (EU) 2022/2555; FISC, 2024)

The inspiration for this thesis came about as a result of conversations with energy industry stakeholders, during which it was mentioned that especially smaller electricity distribution system operators might need assistance in complying with the NIS2 directive. Additionally, for instance Kumar and Mallipeddi (2022) have highlighted the need for more research on how policy regulations can enhance supply chain cybersecurity, whether certifications provided by an external party can supplement government regulations, and what factors influence the effectiveness of these regulations. Nonetheless, the need for a guideline was recognized as the legislation itself does not provide detailed compliance instructions. Thus, the aim for this thesis is to develop a guideline for electricity distribution system operators for complying with NIS2 directive's supply chain aspects by highlighting the special cybersecurity requirements of the DSO's. How this thesis distinguishes itself from other existing recommendations it is sector-specific focusing on the electricity sector supply chain cybersecurity. Thus, it is noted that there already exist unofficial general guidelines from organizations such as Traficom and FISC which were published during the thesis writing period. These recommendations are referred to in this work and used as a basis for forming the guideline. Additionally, there are two other master's thesis works published in Sweden by Linderoth (2024) and in Finland by Fransila (2024). These works are briefly mentioned in this thesis.

This research method for this thesis is design science. The content itself is a case study, focusing on two separate electricity distribution system operators. Data is gathered with

interviews and online surveys from both case companies as well as external experts. This thesis explores different methods for cybersecurity management from both a more relationship-oriented supplier management as well as more technology-oriented product risk aspects. These are the two central themes and levels of knowledge that this thesis is based. As an end product the thesis aims to use design science research as a method for formulating an artefact that is the guideline for NIS2 compliance and general aspects for electricity distribution system operators to consider about cybersecurity in their supply chains.

The guideline is formulated by following research questions:

1. What methods do DSOs have to manage risks at the supply chain level?
2. Which NIS2 factors are the easiest and hardest to manage from the supply chain aspect?
3. How strategically important different information technology and operational technology products are in relation to each other and to the distribution system operators?
4. What is the connection of strategically important products to procurement risk?

The thesis begins with an analysis of the literature aiming to provide a brief overview of cybersecurity problems that are unique to the energy industry. After that, it explores the supply chain elements of the NIS2 directive and how they affect the energy industry, specifically the electrical industry. After that the literature review glances at supply chain cyber risk management and using contracts and relevant standards, as a risk management method. The Kraljic Matrix is examined in the review as an additional tool for supplier risk management. After the literature review, the next chapter covers the research method, design science, that was used for creating the guideline. The method is presented in three phases. The phases consist of both thematic interviews and surveys that were both semi-structured and structured. The data analysis is therefore both qualitative and quantitative. The research results of the analysis are displayed in the results chap-

ter following by the discussion chapter. This chapter addresses the findings' ramifications in light of the previously examined literature. The main findings of the study are outlined in the last chapter, along with their implications for cybersecurity in the energy industry. Based on the findings, recommendations are made, especially with regard to policy, operational plans, and the need for additional research. The limitations of the study are discussed, and areas for future investigation are suggested.

2 Literature review

This thesis begins with a literature review aiming to both introduce the topic as well as gain an understanding of the themes of the research, namely cybersecurity supply chain management of energy sector and how NIS2 is affecting it. The thematic levels that rose from the literature review are on the risk management level: both on the supplier risk as well as product risk level. The first chapter first gives a brief overview of cybersecurity problems that are unique to the energy industry. After that the literature review explores the NIS2 directive focusing especially on the supply chain elements, how the directive affects the energy sector as well as recommendations that have been given to compliance. Following that the literature review focuses the supply chain cyber risk management. A deeper look is taken into using contracts and relevant standards as a cyber risk management method. The Kraljic Matrix is examined in the review as an additional tool for supplier risk management.

This literature review refers to the energy and electricity sector organizations as operators, entities, businesses and organizations depending on the topic of the chapter. When the legal obligations are discussed, the wording is entity, a common legal term referring to a person or organization with separate and distinct legal rights. An operator refers to an individual or an organization who controls and supervises a machinery, for instance distribution system operators control the power grid. Organization is in this context more a business term, i.e. a company where people work towards for the same results. (Cornell Law School, 2022a; Cornell Law School, 2022b; Britannica, 2024)

2.1 Cybersecurity of electricity sector

The cybersecurity of the electricity sector as a part of the critical infrastructure is a topic that is receiving increasing attention. It is noted for instance by the Finnish National Emergency Supply Agency (2022) that the energy sector is made up of various sized business entities with diverse market structures. The cyber maturity level of the sector is generally assessed as good in Finland by the organization. However, the Finnish National

Emergency Supply Agency (2022) has recognized that the energy sector is divided between entities with high and low maturity levels, and the cybersecurity culture varies among these entities. Additionally, it has been identified in Finland that organizations operating over larger geographical areas have invested more in cybersecurity compared to local entities. Since the energy sector includes the electricity sector as a subsector, these evaluations can also be seen to apply to that industry. According to a report made in 2021 by European Union Agency for Network and Information Security (ENISA), smaller businesses may be crucial components of broader supply chains to critical entities such as the electricity sector organizations. The smaller companies in the supply chains are often targeted by cybercriminals. Thus, the cybersecurity management of the whole supply chain can be seen crucial for the critical infrastructure. (Finnish National Emergency Supply Agency, 2022; ENISA, 2021; Durst & Henschel, 2024)

According to the literature, the specific needs of electrical system operators must be considered in the cybersecurity management framework. The electrical system is prone to cascading failures due to its interconnectedness and real-time nature, where a single outage or cyberattack could have far-reaching consequences, such as a blackout. Krause et al. (2021) claim that the key aim of cyber security management in electricity sector is to secure the reliability and resilience of the system. The three fundamental objectives of cybersecurity are to ensure availability, integrity, and confidentiality. In conventional cybersecurity practices, maintaining confidentiality and integrity is typically prioritized, even if it means potentially sacrificing some availability. However, for instance Krause et al. (2021) stress that especially regarding electricity distribution, availability plays a major role as the grid must stay operational all the time. The electricity system has been historically managed by computers out of internet connection, and now with the clash of legacy systems and emerging technologies, new security issues are rising. (ECOFYS, 2017; Krause et al., 2021; Alhelou et al., 2019; Zhou et al., 2020; ECOYS, 2017; Plėta et al., 2020)

2.1.1 Product cyber risk of electricity sector

The ongoing digitalization of the electricity sector highlights the cyber risks linked to the information and communication technology (ICT) products that system operators use. An examination of academic research concerning product risks stresses the difficulties that the industry faces as a result of digitizing electricity sector. Topics like cybersecurity vulnerabilities, reliance on legacy technology, and system interconnection are often discussed in the literature. The conflict between legacy systems and emerging technologies is a recurring theme in the academic literature about the current digitalization of the electricity sector. According to Kumar and Mallipeddi (2022) cybercriminals can get many entry points into systems through the usage of ICT systems. Software vulnerabilities and networked systems are the two primary causes of invasions. (Zhou et al., 2020; ECOYS, 2017; Plėta et al., 2020; Kumar & Mallipeddi, 2022).

The clash of the different technologies used for the operations in the electricity sector is happening due to digitalization that includes a wider use of the internet. Historically, electricity system has been run by computers that were not connected to the internet. The operators of the sector traditionally have been using operational technology (OT) systems that have been isolated from open public networks and information technology (IT) systems separately for different operative purposes. It can be roughly stated that IT technologies include systems that are used for operative tasks related to for instance finance related tasks whereas OT systems contain central systems for power control and operation. However, although the electricity sector is digitalizing, the International Energy Association (2023) argues that the implementation of digital technologies in power grids remains low. Also, researchers such as Monaco et al. (2024) and Borenius et al. (2022) highlight that for example distribution system operators have technical barriers when they need to integrate new systems into existing ones. However, Taylor (2013) notes that operational technology (OT), including two-way communications, intelligent devices, and SCADA, is revolutionizing how distribution systems are monitored and controlled, rapidly changing electric distribution operations. Similarly, information technol-

ogy (IT) continues to impact distribution operations with ongoing advancements in mobile technologies, analytics, systems integration, and computing platforms. Both of these systems are expected to become more blended, meaning that for instance traditional OT products start having IT product features. Thus, according to Borenius et al., (2022) it has become more complicated to separate the different technologies from each other, especially as they are merging. (IEA, 2023; Monaco et al., 2024; Borenius et al., 2022; Taylor, 2013; Palo Alto Networks, 2024)

The merging, often referred to as "IT-OT convergence" can be defined as the integration of information technology (IT) data management systems with operational technology (OT) industrial systems. However, for instance Maleh (2021) argues that in addition to providing a true competitive advantage, the convergence of these two universes has a drawback in the form of cyberattacks. Nonetheless, the literature generally admits that information and communication (ICT) technology is essential to electricity distribution operators and other energy sector stakeholders. Therefore, it has been stated, that conventional IT methods of cybersecurity are not applicable to all cybersecurity issues regarding the electricity distribution. The new level of interconnected operational technology necessitates cybersecurity measures. The cyber threats can extend all the way to the product component level. (IEA, 2023; Monaco et al., 2024; Borenius et al., 2022; Michalec et al., 2023; Upadhyay & Sampalli, 2019; Maleh, 2021; U.S. National Institute of Standards and Technology, 2024)

As the sectors of critical infrastructure are becoming evermore interconnected and prone to cascading failures due to that, the European Union has decided to enhance its cybersecurity policies (European Commission, 2024a). The next chapters of the literature review are focusing specifically on The Revised Network and Information Security Directive (NIS2), how the supply chain cybersecurity is addressed in the directive as well as how the directive is affecting the energy sector.

2.2 The Revised Network and Information Security Directive

The Revised Network and Information Security Directive (Directive (EU) 2022/2555) is part of EU's cybersecurity strategy, aimed at improving the cyber safety of critical infrastructure consisting of essential and important service providers. The directive, abbreviated as NIS2, entered into force on January 16th of 2023. The member states of European Union (EU) must implement NIS2 into national legislation by October 18th of 2024. The NIS2 Directive expands upon the foundation of the original NIS1 Directive (2016/1148) that was the first component of EU cybersecurity legislation. The revised directive has a wider scope, it includes categorization of essential and important entities, a size-threshold rule, harmonized security requirements, incident reporting, supervision and enforcement, penalties and new risk management obligations, such as addressing the supply chain security. The legislative proposal in Finland would implement the risk management aspects of NIS2 as a new law in Finland, a law of risk management of cybersecurity. (Directive (EU) 2022/2555; Sievers, 2021; SANS, 2024; Finnish Government, 2024)

Compared to the previous Network and Information Security Directive (NIS1) the revised directive covers a wider range of entities and broadens the scope already introduced in NIS1. In NIS1, the entities were identified as "operators of essential services" and "digital service providers" (Directive (EU) 2016/1148). This categorization is superseded by a new categorization in the scope of NIS2. The entities are now classified either as "important" or "essential". Essential and important sectors have a different obligation scope. Additionally, compared to the previous directive, NIS2 introduces more sectors to it range. The essential sectors, i.e. "sectors of high criticality", are energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), public administration and space (Directive (EU) 2022/2555). Other important sectors, i.e. critical sectors, i.e. important sectors are postal and courier services, waste management, chemical business, food business, manufacturing and digital providers (Directive (EU) 2022/2555) . (Directive (EU) 2016/1148; SANS, 2024; Sievers, 2021; European Commission, 2023; Directive (EU) 2022/2555).

In NIS2 Directive it is designated that entities defined as essential face stricter requirements compared to important entities. Essential entities face higher financial penalties for non-compliance as well as are in a stricter scope of regulatory oversight. Essential entities are subject to both proactive and reactive supervision defined as ex ante. In contrast, important entities are only subject to reactive supervision, ex post. However, the cybersecurity requirements are the same for both entities. In the revised directive some of the obligations for the entities are defined by the size-threshold rule. Companies must independently assess whether they fall under the jurisdiction of NIS2 in order to comply with the size threshold rule. Previously, government officials' decisions determined which companies were required to adhere to NIS1 obligations. Size threshold rule is applied aligning “Commission Recommendation of concerning the definition of micro, small and medium-sized enterprises” (2003/361/EY). Medium-sized enterprises have minimum 50 employees or an annual return and a statement of financial position exceeding EUR 10 million. "Large companies" have at least 250 employees, an annual return over EUR 50 million, and a statement of financial position total above EUR 43 million. Small and micro businesses are generally outside the scope unless their business is defined of exceptionally relevant to the directive. (European Commission, 2023; FISC, 2024; Sievers, 2021; Finnish Government, 2024; European Commission 2003/361/EY).

The revised directive presents a range of cybersecurity risk management measures, including “supply chain security and the security of network and information systems acquisition”, which are specifically outlined in Article 21 of NIS2. The Recital (85) and Article 21 part (d) and (e) of the directive are the ones that are specifically relevant for this thesis as it focuses on the supply chain management aspect of NIS2. Therefore, this literature review part is focusing on especially on Recital (85) and Article 21.

2.2.1 Recital (85)

A recital is an explanation of facts or justifications for the existence of a law or contract. In NIS2, the Recital (85) focuses on the importance of addressing cybersecurity threats

that result from a company's supply chain and supplier relationships, particularly those posed by third-party suppliers. The recital highlights the importance it is in light of the frequency of incidents in which organizations have fallen victims to cyberattacks and in which malicious actors have compromised the security of an organization's network and information systems by taking abuse of the flaws affecting the products or services provided by third parties. (Termly, 2024; Directive (EU) 2022/2555)

> *Essential and important entities should therefore assess and consider the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers. (Directive (EU) 2022/2555)*

Recital (85) in NIS2 proposes integrating cybersecurity risk management into the contracts that organizations have with the vendors of their devices. According to Van ’t Schip (2024) this should encourage the entities to invest in cybersecurity. The actors who produce the products, i.e. the suppliers, may require sufficient supply chain cybersecurity in order to continue selling their products and adhere to these agreements. These requirements have the possibility to extend even further than to the first vendor, as recital (85) states “those entities could consider risks stemming from other levels of suppliers and service providers” (Directive (EU) 2022/2555) . (Van ’t Schip, 2024; Directive (EU) 2022/2555)

2.2.2 Article 21 (d) and (e)

The Article 21 part 1 of the directive mandates that the EU member states make sure that the entities defined as essential and important implement “appropriate and proportionate” technical, operational, and organizational risk management methods. The objective of these methods is to mitigate the cybersecurity risks that are posed to the security of the network and information systems these entities use for their own operative processes or when delivering the services to customers or users. The proportionality

of the utilized measures should be assessed through the level of how the entity is exposed to risks, what is the size of the entity organization, what is the likelihood of the incidents to occur and what would be the severity including the impact on society and the economy. (Directive (EU) 2022/2555)

NIS2 introduces various measures for cybersecurity risk management such as supply chain security and security in network and information systems acquisition. These are separately defined in Article 21 part 2. The NIS2 Directive emphasizes that the risk management measures should follow an all-hazards approach. This approach is aiming to protect both network and information systems and their physical environment from incidents. The all-hazard approach includes a list of measures that the entities need to implement. These measures are listed from (a) to (j):

> *(a) policies on risk analysis and information system security;*
> *(b) incident handling;*
> *(c) business continuity, such as backup management and disaster recovery, and crisis management;*
> *(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;*
> *(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;*
> *(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;*
> *(g) basic cyber hygiene practices and cybersecurity training;*
> *(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;*
> *(i) human resources security, access control policies and asset management;*
> *(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate. (Directive (EU) 2022/2555)*

Point (d) and (e) of Article 21 can be seen particularly relevant measure to supply chain and supplier management as well as the cybersafe procurement of products. Point (d) measure is “supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers” and point (e) measure “(e) security in network and information systems acquisition, development

and maintenance, including vulnerability handling and disclosure". (Directive (EU) 2022/2555)

The third paragraph of Article 21 also mandates that entities must consider "the specific vulnerabilities of each direct supplier and service provider", as well as "the overall quality of their products and cybersecurity practices", including their "secure development procedures". Member States must ensure that, when determining the appropriate measures, entities consider the outcomes of "coordinated security risk assessments of critical supply chains conducted in accordance with Article 22(1)". Van 't Schip (2024) argues that this collaboration could be achieved by utilizing standards such as provided by International Organization for Standardization (ISO). (Directive (EU) 2022/2555; Van 't Schip, 2024)

However, according to Ferguson (2023), a statutory interpretation states that the goal of NIS2's risk management measures is to minimize the impact of cyberattacks on systems and services rather than prevent every attack. The goal is therefore to maintain system functionality; the most important aspect is that the systems can recover and keep operating. Van 't Schip (2024) further supports this claim by declaring that the flexible NIS2 cybersecurity risk management approach places a strong emphasis on cyber resilience. In this context, cyber resilience means the ability of an organization to quickly recover from an attack and prohibit any further problems. Van 't Schip (2024) writes also that the entities must constantly adjust to distinctive risks and characteristics of the supply chain in order to avoid relying on generic risk assessments for the devices they use in their supply chains. (Ferguson 2023; Van 't Schip, 2024)

2.3 Recommendations for NIS2 supply chain management

Recommendations regarding the directive, for instance those from the Finnish Transport and Communications Agency (Traficom) and the Finnish Information Security Cluster (FISC) have provided general recommendations for NIS2 compliance, and these also handle the organizational supply chain aspect addressed e.g. in Recital (85) and Article 21.

However, there are not many academic references about the topic. This is probably because this thesis was mostly written in early 2024, before the directive is fully incorporated into national law. Therefore, the previously mentioned references are mostly cited in this chapter.

According to NIS2 directives supply chain aspects the organizations referred to as entities "should" evaluate and consider "the resilience and quality of their products and services" as well as the cybersecurity risk-management strategies incorporated into these products and services. They should also evaluate the secure development procedures and cyber-security policies of their service providers and suppliers. These organizations might take into account risks arising from different levels of suppliers and service providers. Both the relationships in the supply chain management as well as the operative aspects such as procurement and product lifecycle management should be considered. These aspects are covered for instance in the recommendations provided by Traficom and FISC that are discussed next. (Directive (EU) 2022/2555)

2.3.1 Recommendations given by the Finnish Transport and Communications Agency and the Finnish Information Security Cluster

Traficom (2024) and FISC (2024) have both made draft recommendations on how companies should comply with the cybersecurity risk management measures mandated under the NIS2 Directive. The recommendations are very similar to each other. According to FISC (2024), a good general rule of thumb is to think about what forms of control, surveillance, and resilience would be appropriate if the company's employees were in charge of the tasks that the third-party supplier performs. The recommendation provided by Traficom explicitly outlines which industry standards it has used to make the recommendation. One of them is ISO27001 by example. Therefore, it can be assumed that also FISC is using the same standards as a framework for providing the recommendations. (Traficom, 2024; FISC, 2024)

Table 1. Key recommended measures to comply with NIS2 requirements of supply chain and supplier management. (Traficom, 2024; FISC, 2024)

Key recommended measures to comply with NIS2 requirements of supply chain and supplier management
Listing all suppliers and subcontractors that have an effect on the cybersecurity.
Making a risk management model according to the list with an all-hazard approach. Assessing the suppliers through the model.
Assessing and considering the suppliers and service providers cybersecurity practices.
Set and document requirements for cybersecurity in contracts.
Considering cybersecurity risks of complete supply chain.

The table above lists the key recommended measures to comply with NIS2 requirements of supply chain and supplier management given by the Finnish Transport and Communications Agency (2024) and the Finnish Information Security Cluster (2024). Listing all suppliers and subcontractors that have an effect on the cybersecurity is where both of the organizations, Traficom (2024) and FISC (2024) recommend to start. The entity should identify which of its suppliers are in a key role in its supply chain. These suppliers should be listed including the suppliers contact information and a description of each supplier's systems, services and goods which are relevant to the buyer entity. Additionally, Traficom (2024) advises adding contract-related details to the listing, such as the agreement's duration and life cycle-related matters. According to FISC (2024) this listing should include description of the supply chain, which includes the interdependencies of the actors, the identified vulnerabilities and threats contained in the services and the effects of the identified risks extending to subcontractors. (Traficom, 2024; FISC, 2024)

The second recommendation that can be derived from Traficom and FISC (2024) is that the listing described in previous paragraph should be used in making a risk management model with an all-hazard approach. The entities should then assess suppliers through the risk management model. A starting point in this step is that the entities should go through the listing one by one and assess that if a supply chain disruption happened to a partner in the listing, how it would affect the buyer entity's operations. After that, according to Traficom (2024) the entity should choose risk management measures that fit the supply chain and execute the measures to those suppliers, in the situation when

risk management measures have a cybersecurity-promoting effect. FISC (2024) recommends to use a basic model of information security as a reference framework for the evaluation. FISC (2024) also recommends to organize suppliers according to the risk level, the so-called risk category. The risk category consists of at least two aspects: the importance of the supplier to the company's (or entity's) own operations and the available information on the supplier's own risk management. (Traficom, 2024; FISC, 2024)

The available information about the supplier's risk management method should serve as one key component for complying with NIS2 supply chain management methods according to both Traficom (2024) and FISC (2024). Traficom (2024) suggests considering the risk management methods and cybersecurity policies that the supplier is already implementing. When the entity is applying its risk management measures, it should consider supplier-specific vulnerabilities, the quality and resilience of the products and risk management methods, services and policies, certifications and other evidence provided by the supplier. The vulnerabilities can rise from location, product range or the nature of the industry. (Traficom, 2024; FISC, 2024)

When the necessary risk assessments are done, the entity should set and document requirements for cybersecurity in contracts. The entity should identify cybersecurity-related features that are important to them and set proportionate requirements. These may include, for example, service level agreements to be set in contracts. The entity should include cybersecurity risk management procedures in contracts with direct suppliers and service providers, per both Traficom (2024) and FISC (2024). FISC (2024) separately emphasizes that there is no reason to transfer the requirements of the legislation to the supplier in the style of "the supplier must meet the requirements of the NIS2 directive". Operators can also deal with risks arising from subcontractors of primary suppliers, i.e. from the next levels of the value chain. However, it is good to remember that each supplier is responsible for its own risks independently and, if necessary, sharing risk information in the value chain. When an operator acquires outsourced services, it is important to understand the level of information security required for its own services and

the service provider's ability to deliver a sufficiently secure service in accordance with these requirements. Contractual means can be used to be ensured about the procurement safety. This can be applied by examining the product characteristics, by requiring certifications, by ensuring the reliability of the supplier and by preparing for risks. Safety requirement should already be defined in the early stages of procurement and the requirements have been delivered to suppliers and incorporated into the contract. (Traficom, 2024; FISC, 2024)

Both organisations emphasize that it would be recommendable that the entity would consider the cybersecurity risks of the complete supply chain. When choosing suppliers and service providers, the supplier should to take into account the statement made by the member state's supervisory body regarding the outcomes of the risk assessment. The operator could also request a component list of critical products and ser-vices (e.g. SBOM, software bill of materials, HWBOM, hardware bill of materials) if necessary to identify and manage dependencies and vulnerabilities against them. (Traficom, 2024; FISC, 2024)

According to FISC (2024) when an entity procures services or products the requirements of the cybersecurity should be well defined and communicated. This is justified with also the matter that it is easier for suppliers to answer to quotation requests when the operator knows how to explain their information security needs in a sufficiently comprehensive and clear manner. Traficom (2024) outlines that the entity should be prepared in changes in the contracts they make. These changes could entail for example changes in ownership, or changes regarding the service providers. If would be beneficial for the entity that if possible, the service or resource could he transferred or returned to the entity’s own control. (FISC, 2024; Traficom, 2024)

2.3.2 Recommendations for NIS2 supply chain management and ISO27001

Various authorities, such as Traficom (2024), have implemented for instance ISO27001 practices to their recommendations for companies to meet NIS2 requirements. The legislative framework and the security standard are in fact similar in some terms. Both address risk assessment, incident response, and continuous improvement. The key distinction is that while NIS2 focuses on critical sectors, ISO27001 is applicable to all kinds of organizations. While NIS2 places particular legal obligations on organizations falling under its jurisdiction, ISO27001 does not mandate legal compliance. One key difference is also that whereas NIS2 has requirements for reporting incidents to the appropriate authorities, ISO27001 does not have a mandatory reporting element. Therefore, ISO27001 is not a complete tool to comply with NIS2 requirements. Nevertheless, when searching online about NIS2 compliance, ISO27001 is a standard that comes up in the search the most often. Although not many academic references are made about the similarities of the standard and the directive, for instance Van ’t Schip (2024) argues that the ISO standards can be used in order to comply with NIS2. Additionally, Fransila (2024) has written in his thesis that the ISO27001 standard is one tool to comply with the legislation. (Traficom, 2024; Privacyengine, 2024; Van ’t Schip, 2024; Fransila, 2024)

The supply chain is emphasized heavily in the NIS2 directive as a crucial element of cybersecurity risk management. This emphasis is particularly relevant to the electrical industry, given the growing recognition of supply chain vulnerabilities as important sources of risk. How the directive affects the energy, especially electricity sector, is explored in the next chapter.

2.4 The Revised Network and Information Security Directive for electricity sector

The needs for cybersecurity are becoming more specialized across all sectors of the energy industry. The European Union has recognized the energy sector as part of the critical

infrastructure, and as such, the industry is subject to new legislative requirements. Two directives, the Revised Network and Information Security Directive (NIS2, Directive (EU) 2022/2557) and the Directive on the Resilience of Critical Entities (CER, Directive (EU) 2022/2555), put more pressure for energy sector operators, referred to as “entities” in legal terms, to enhance their cybersecurity measures. The CER Directive introduces a framework through which entities of critical infrastructure can be identified. Energy sector along with its subsectors is identified as highly critical. The organizations that fall under the subcategory of critical infrastructure sectors are referred to as entities of critical infrastructure. The energy subsectors are electricity, oil, gas, district heating and cooling, and hydrogen. Distribution system operators are defined as a part of the electricity sector in the scope of the entity. These entities are subject to especially strict compliance requirements. They are also mandated to comply with the NIS2 Directive's cybersecurity requirements. These organizations have to incorporate the legislative cybersecurity requirements into their operations. The requirements include risk management measures, such as supply chain cyber risk management. The shift in the legislation from the concept of “critical infrastructure” (CI) to “critical entity” (CE) is according to Pursiainen and Kytömaa (2022) also an ideological in terms that the European union now aims to target specific operators inside the sector of critical infrastructure instead of targeting the entire sector. As an example, now the legislation targets individual electricity distribution system operators instead of the whole electricity sector. Thus, according to them it can be seen as a fundamental change about managing critical systems. (European Commission, 2023; European Commission, 2024b; European Commission 2024c; Directive (EU) 2022/2555; Directive (EU) 2022/2557; Finnish Government, 2024; Pursiainen, & Kytömaa, 2022)

The electricity sector consists of companies of varying size: therefore, the size-threshold rule is stricter for some. The energy sector entities are defined as essential entities in NIS2. Therefore, the sector operators need to adhere to stricter rules. The energy sectors subsectors covered by the NIS2 Directive are electricity, oil, gas, district heating and cooling, and hydrogen. Electricity distribution system operators are defined as a part of the

sector of electricity in the scope of the entity. Electricity distribution operator companies vary of size: therefore, the size-threshold rule is stricter for some. One thing that seems interesting is also that distribution system operators, for example, have a monopolistic position in the electricity distribution of a country level, whereas many competing enterprises can create services and digital products. Smaller operators that serve municipalities and fewer consumers play a significant role in Finland's electricity distribution network, despite the fact that larger companies dominate the market. This emphasizes the significance of also the smaller organizations in the resilience of the sector. (Finnish Government, 2024; Finnish Energy 2024a)

The master's thesis written by Linderoth (2024) is exploring how NIS2 affects the energy sector in Sweden. Based on the findings, it appears that management's increased attention to and participation in information security matters is the largest organizational shift that occurs with the implementation of NIS 2. Additionally, it appears that maintaining supply chain compliance with NIS 2 is the most significant challenge the industry will face. Furthermore, the thesis confirms that small businesses lack the resources required to meet the new NIS 2 requirements. (Linderoth, 2024)

Given that the electricity distribution system operators under focus in this thesis vary in size, it is crucial to consider the differing challenges and opportunities faced by companies of different scales. This aspect of company size is a significant factor that can influence operational strategies, resource allocation, and overall system performance, making it an important dimension for analysis in this thesis as well.

2.5 Cyber supply chain risk management

Cyber risks to the energy industry as a whole have been escalating during the past years, one of the most famous cases being the Ukraine grid hack in 2015. Borenius et al. (2022) and Saberi et al. (2019) emphasize that the electricity sector must address the expanding number of supply chain cyber-attacks by implementing security measures across the

whole supply chain. Borenius et al. (2022) argues that the increased utilization of solutions for managing the electricity grid that are based on software solutions can make supply chain attacks more likely to occur. These attacks are becoming increasingly prevalent and difficult to prevent as a multitude of organizations are involved in the supply chain. According to Yeboah-Ofori and Islam (2019), the supply chain organizational environment has made cyber security a significant challenge because of the integration and interdependencies of multiple stakeholder systems that are interconnected to accomplish organizational objectives. Hence, the following subchapters of the literature review delve into the topic of supply chain management, supplier relationship management and procurement from a cybersecurity aspect. (ISA, 2017; Borenius et al., 2022; Yeboah-Ofori & Islam, 2019; Saberi et al., 2019)

2.5.1 Key terminology of supply chain cybersecurity

Understanding fundamental ideas such as supply chain management and supplier relationship management is essential when discussing cyber supply chain risk management, particularly in industrial sectors that rely heavily on multifaceted supply chains. Mentzer et al. (2001) define supply chain management (SCM) as the coordinated management of business functions and tactics within a company and across its supply chain. According to the authors, enhancing long-term performance for each company and the supply network as a whole is the aim of supply chain management. Different business functions carry out activities such as procurement, i.e. the act of buying products and services. The operations can also be outsourced, which means using an outside supplier for any value chain function. These activities amongst others involve supplier relationship management (SRM). According to for instance Moeller et al. (2006) SRM involves activities aimed at building and improving value within the supply chain relationships. These activities are keeping an eye on out-suppliers and building, maintaining, and ending relationships with in-suppliers. Supply chain risk management has been defined by Tang and Tomlin (2008) as “the management of supply chain risks through coordination or collaboration among the supply chain partners so as to ensure profitability and continuity.” (Yeboah-

Ofori & Islam, 2019; McKinsey, 2024; Mentzer et al., 2001; Moeller et al., 2006; Teece, 2016; Tang & Tomlin, 2008)

There are also specialized terms specifically related to managing cyber threats and preventing attacks within the supply chain. According to the definition of ENISA (2021), a supply chain attack involves at least two linked attacks. It starts with an attack on a supplier, then uses the compromised supplier to target another entity, such as the final customer or another supplier, to access its assets. In order for an incident to be defined as a supply chain attack, both the supplier and the customer need to be targeted. Cyber supply chain risk management (CRSM) is a process of utilizing different methods to mitigate these cyber threats in the supply chain, as defined by Boyson (2014). These methods vary from risk assessments to contractual methods. Methods for controlling, managing, and improving the supply chain system are known as supply chain cybersecurity techniques. They are implemented to guarantee security of information, safeguard products, and maintain business continuity. (ENISA, 2021; ECOFYS, 2017; Boyson, 2014; Yeboah-Ofori & Islam, 2019)

2.5.2 Supplier relationship management in cybersecurity

There are different risks associated to cyber supply chain management. Examples of these relate e.g. to procurement and IT outsourcing. Pereira et al. (2017) and Traficom emphasize the need of cyber risk management when procuring ICT. Traficom (2024) argues that inadequate arrangements in the procurement process increase the likelihood of numerous threats, including vendor lock-in, threats arising from ownership changes, loss of knowledge, and loss of the acquired product. Additionally, Benaroch (2020) states IT outsourcing (ITO) significantly increases cybersecurity risk exposure. When organizations delegate their IT and cybersecurity responsibilities, they often presume that the responsibility for managing cybersecurity risks shifts to the ITO providers. However, in practice, the risk profile of these organizations does not merely transfer but expands to include both their own risks and those introduced by their ITO providers. According to

the National Audit Office of Finland (2023), managing contracts for old information systems can present specific challenges. Sometimes, reliance on a single supplier is due to market conditions or procurement processes according to the authority. Generally, it can be outlined that avoiding vendor lock-in, where a buyer is dependent on one supplier, is considered important. (Pereira et al., 2017; Traficom, 2024; Benaroch, 2020; National Audit Office of Finland, 2023)

The risks related to cyber supply chain management can be reduced by different methods, such as quality assessments, third-party auditing, utilizing and requiring standards in contracts and aligning interests and cooperating with stakeholders within the supply chain. Borenius et al. (2022) state that in order to essentially decrease the supply chain attacks, buyers consider the general quality of the products and the cybersecurity measures of their suppliers, including safe development processes. According to Yeboah-Ofori and Islam (2019) supply chain parties should implement their security processes in accordance with international standards and conduct regular audits by third parties in order to guarantee appropriate control and mitigation methods in the cyber supply chain. Cooperating within the supply chain regarding the cybersecurity issues has been deemed to be beneficial by multiple academic researchers. According to Kumar and Mallipeddi (2022) for instance sharing data, resources, and profits or costs among the parties involved in the supply chain are examples of coordinating the supply chain interests. According to Aichbauer et al. (2022, p.13) a modern approach to leadership in procurement is where suppliers will be seen as partners. (Borenius et al., 2022; Yeboah-Ofori & Islam, 2019; Aichbauer et al., 2022, p.13)

Considering the preceding paragraph, according to academics, proper risk management measures including cooperation within the supply chain seem are the keys to appropriate cyber supply chain risk management. According to Verlag (2013), inadequate client-vendor relationship governance is the reason behind many IS outsourcing projects' inability to produce the anticipated benefits. Earlier research has primarily examined relational or contractual governance, frequently viewing them as substitutes. This implies

that a contract may reduce the requirement for a relationship built on trust and vice versa. Combining the two kinds, though, may according to for instance Verlag (2013) result with more advantages. Boyson (2014) presents different methods of procedures to take during the supplier contract life cycle. Firstly, pre-contract coordination efforts include incorporating clauses into contracts with vendors requiring them to handle cyber risk. Midway through the lifecycle, a formal contract with the vendor specifies how mitigation measures based on time are to be carried out. Compliance is then evaluated through a vendor rating system. (Verlag, 2013; Boyson, 2014)

As stated in the previous paragraphs, standards and contracts serve as a cyber risk mitigation method. They are also considered in the NIS2 directive. Therefore, the next chapter is looking into standards and contracts on a deeper level.

2.6 Standards and contracts as cyber risk mitigation

Complying with the NIS2 Directive requires risk management in supply chain and supplier relationship management. Organizations like Traficom and FISC advise including safety clauses in contracts and using global standards to comply with NIS2 requirements. Additionally, there are many research articles where standards and contracts are seen as a vital part of supplier cyber risk mitigation. According to Taherdoost (2022cybersecurity standards establish the guidelines that a company must adhere to in order to meet cybersecurity goals and reduce cyberthreats. Contracts are official agreements that specify conditions, such as when a buyer requires a supplier to follow a certain cybersecurity standard. As stated by Dubey et al. (2018), contracts serve as the foundation in the procurement process to establish both communication and relationship management and between the buyer and the supplier. (Traficom, 2024; FISC, 2024; Taherdoost, 2022; Dubey et al., 2018)

Purset et al. (2014) explain that the goal of applying cybersecurity standards is to decrease the likelihood of cyberthreats to avoid or eliminate cyberattacks. Cybersecurity

standards, which outline specified technical processes and sets of practices, are designed to help organizations protect their cyber operating environments. These standards provide a framework for measuring an organization's management and operational practices against specific requirements. As Heras-Saizarbitoria and Boiral (2013) put it, standards establish the minimum acceptable level of performance or quality, as well as the optimal level an organization must meet to be considered compliant. To demonstrate compliance with a standard, a company can undergo certification by an external third party. Following certification, the company's operations can be externally assessed through audits to ensure that they adhere to the standards. (Purset et al., 2014; Syafrizal et al., 2020; Heras-Saizarbitoria & Boiral, 2013; Finnish Standards Association, 2024).

Information security standards and information security governance standards are the two primary categories into which cybersecurity standards are typically divided. According to Syafrizal et al. (2020) choosing a standard or framework ought to be determined by the specific requirements of the organization to ensure they adequately meet the business's needs. The implementation of the standard should go hand in hand with a cybersecurity framework. While cybersecurity frameworks serve as general guidelines that include several elements or domains that can be implemented by organizations, they do not determine the steps that must be taken. In contrast, cybersecurity standards lay out the measures sequentially, pointing out what is anticipated to be done throughout the process, and clearly state out the measures that align with the standard. Therefore, for instance Antunes et al (2022) recommend that if a company is adopting a framework it should offer a general structure and methodology in addition to describing the processes for implementation, evaluation, and scope. (Taherdoost, 2022; Syafrizal et al., 2020; Antunes et al., 2022).

Cybersecurity standards are widely recommended by academic scholars as effective methods for managing risks within the cyber supply chain. Yeboah-Ofori and Islam (2019) explain that to ensure cyber supply chain controls and adequate mitigation techniques, it is anticipated that all parties of the supply chain make sure that there is a regularity in

third-party auditing and that the already implemented security policies align with international standards. This can be outlined in clauses set in contracts. Calder (2008) states that, certification builds trust with clients by demonstrating effective information security practices and Hamdani et al. (2021) argue that if a supplier utilizes a standardized approach to risk management, it is easier for the buyer to assess its compliance. Buccafurri et al., (2015) state that compliance analysis is crucial for security management. By implementing security measures that ensure requirements are met, compliance analysis aims to enhance service quality and reduce vulnerabilities that may arise from non-compliance risks. (Yeboah-Ofori & Islam, 2019; Calder, 2008; Boyson, 2014; Hamdani et al., 2021; Buccafurri et al., 2015)

However, there are also intersecting opinions about supply chain cybersecurity risk management methods. For example, Song et al. (2024) have investigated that requiring a cybersecurity assurance could encourage a supplier to carry out cursory actions. According to Song et al. (2024) there is a possibility that If a supplier estimates security effort without knowing the cybersecurity level of maturity anticipated by the buyer, the likelihood of the pointless actions is reduced. The writers also argue that the buyer should to hold the supplier more accountable for security breaches. (Song et al., 2024)

Kanstren et al. (2017) have studied in Finland that in the industry certifications play an essential part in explicating the cybersecurity requirements. The authors argue that the importance is particularly relevant due to the current trend of businesses outsourcing IT and cybersecurity services. Kanstren et al. (2017) explain that the procured end products are often built of extensive chains of subcontractors and integrations of their subsystems. These tend to lead to additional external dependencies in the supply chain. Beyond certifications, there is significant emphasis on demonstrating a functioning system behind the certificate. Certifications such as those based on for example ISO 27000 and industry best practices are seen as vital tools for managing numerous vendors and subcontractors with varying security procedures. (Kanstren et al., 2017)

ISO27001 is also referred to many times when talking but NIS2 compliance, for example in the recommendations by the Finnish authorities Traficom and FISC referred to earlier.

2.6.1 ISO27001 role in NIS2 compliance

There are numerous cybersecurity standards, one of the most well known for information security management systems being ISO27001. According to the International Organization for Standardization (ISO), ISO27001 provides a tool for risk-management, cyber-resilience and operational excellence. Humphreys (2008) argues that the standard has evolved into the "common-language" for managing information security. Although it is stated in NIS2 Directive that ISO27001 standard is required for complying with the directive, using ISO27001 standard for compliance is recommended by various authorities. For example, Traficom (2024) has ISO27001 practices to their recommendations for companies to meet NIS2 requirements. (Calder, 2008; Humphreys, 2008; Traficom, 2024)

The NIS2 legislative framework and the security standard are in fact similar in some terms. Both address risk assessment, incident response, and continuous improvement. The key distinction is that while NIS2 focuses on critical sectors, ISO27001 is applicable to all kinds of organizations. Also, NIS2 places particular legal obligations on organizations falling under its jurisdiction but ISO27001 does not mandate legal compliance. One key difference is also that whereas NIS2 has requirements for reporting incidents to the appropriate authorities, ISO27001 does not have a mandatory reporting element. Therefore, ISO27001 is not a complete tool to comply with NIS2 requirements. Nonetheless, according to Nowak (2015), the ISO 27001 for a supply chain is only a starting point for ensuring that the proper protocols are in place when it comes to information security. The riskiest relationships frequently call for greater disclosure or more stringent regulations. These might be for example reporting more frequently. (Privacyengine, 2024; Nowak, 2015)

Despite the fact that contracts and standards are often researched as ways to manage cyber risk for suppliers, other tools like the Kraljic matrix, discussed in the next chapter, can also be used to assess suppliers.

2.7 Supplier risk assessment with Kraljic matrix

Though Kraljic matrix is not a common tool to assess cyber risks it is included in this literature review. This chapter is referring to especially articles by Caniëls & Gelderman (2005) and Hajmohammad and Vachon (2016) as they are well-cited, they both have explained how the matrix can be utilized as well as given recommendations how to apply the matrix into supplier risk assessment. As it has been stated e.g. by Verlag (2013), inadequate client-vendor relationship governance is the reason behind many IS outsourcing projects' inability to produce the anticipated benefits. Therefore, Kraljic matrix can be used for supplier risk assessment by defining the strategic importance of different suppliers. (Verlag, 2013; Caniëls & Gelderman, 2005)

Created by Peter Kraljic in 1983, the Kraljic Matrix is a supply chain strategic management tool created to help companies analyse and manage their procurement portfolio based on the risk and profitability of their sourcing activities. Kraljic matrix is often referred to as Kraljic purchasing portfolio or Kraljic portfolio matrix. The aim of Kraljic matrix is to help decision making by enabling firms to prioritize their purchasing strategies products and services based on "supply risk" and "profit impact". (Caniëls & Gelderman, 2005; Garzon et al., 2019; Kraljic 1983 in Caniëls & Gelderman, 2005)

Figure 1. Kraljic purchasing matrix modified from article by Caniëls & Gelderman, (2005)

The picture above showcases a simple version of the Kraljic matrix. The profit impact is in the y-axis whereas the supply risk in the horizontal x-axis. The original work by Kraljic focuses on strategic products, but this gap has been filled by other scholars and tasks for bottleneck, non-critical and leverage items have been defined. Zsidisin (2003) defines supply risk as the likelihood of an incident occurring due to failures by individual suppliers or disruptions in the supply market. According to the writer, supply risk that has materialized can be leading to outcomes that prevent the purchasing firm from meeting customer demand or pose threats to customer lifecycle or safety. As Caniëls & Gelderman (2005) explain, profit impact in the matrix is according to how much a product or a service contributes to the profitability of the company. It is possible to start conducting supplier risk assessment according to Kraljic matrix by first listing all the products and services procured by the organization. After that the products are classified into a two-by-two matrix, like in the picture showcased above, based on their profit impact and supply risk. Based on these two dimensions, Kraljic Matrix divides products and services in four groups: strategic items, leverage items, bottleneck items and non-critical items. (Caniëls & Gelderman, 2005; Zsidisin, 2003; Ye, 2021)

The box for strategic items is located in the upper-right corner of the image because it represents the highest profit impact and supply risk. Due to these factors the strategic items are crucial to organizations. Examples of strategic items include for instance engines for car manufacturers or turbines for the chemical industry, often sourced from a single supplier, increasing supply risk. According to the Kraljic matrix philosophy, in order to manage these risks, organizations should form strategic partnerships with suppliers. According to Caniëls and Gelderman (2005), the best course of action is to keep up strategic alliances with suppliers rather than ending existing ones. The same authors state that upholding strategic partnerships has benefits that align with the Kraljic matrix, including the reduction of supply risks through mutual trust and commitment and improvement of product quality, reliability of delivery, and cost savings. Hajmohammad and Vachon (2016) suggest that supply managers choose a collaborative-based risk mitigation strategy in a situation where the supplier risk is perceived high. This mitigation strategy would entail dealing directly with the suppliers and developing solutions collaboratively. (Caniëls & Gelderman, 2005; Hajmohammad & Vachon, 2016)

In the lower-right corner is the box for bottleneck items that also have a high supply risk but a lower profit risk compared to the strategic items. Bottleneck items are vulnerable to supply constraints, but they have relatively little effect on a company's financial performance. For these products, suppliers hold a dominant power position. Caniëls & Gelderman (2005) suggest that the purchasing organization accepts their dependence of the bottleneck items and focus on mitigating the negative impact of a situation possibly deemed unfavourable. Common strategies in this situation is to for example maintain extra stocks and seeking to reduce dependence by finding other suppliers or broadening product specifications to ease the transition out of unfavourable positions. According to Kraljic's model Hajmohammad and Vachon (2016) recommend ensuring the supply for the bottleneck items even at higher prices. (Kempeners and van Weele, 1997 in Caniëls & Gelderman, 2005; Caniëls & Gelderman, 2005; Hajmohammad & Vachon, 2016)

On the left side of the picture, leverage items are located in the upper-left corner of Kraljic matrix. Leverage items pose a relatively low supply risk but have a high profitability impact for the company. They are typically sourced from multiple suppliers and constitute a large portion of the end product's cost but carry low supply risks. Caniëls & Gelderman (2005) claim that position allows buyers to exploit their buying power through competitive bidding and coordinated purchasing strategies. Alternatively, buyers may develop strategic partnerships with technologically advanced suppliers to enhance competitive advantages. Hajmohammad and Vachon (2016) advise that with leverage items, if supply managers believe there is little risk associated with them, they could impose their sustainability-related demands on dependent suppliers. However, if the buyers sense a higher degree of supplier sustainability risk, the buyers could adopt a cooperative measure to implement sustainability standards at suppliers' facilities. According to Hajmohammad and Vachon (2016), initially, this approach might be costlier than simply cutting off suppliers. However, in the long term, it could be beneficial as it helps maintain a larger pool of suppliers. (Caniëls & Gelderman, 2005; Hajmohammad & Vachon, 2016)

Lastly, on the lower-left corner are the non-critical items. Non-critical items tend to have low value per unit and minimal technical or commercial issues. Caniëls & Gelderman (2005) explain that the non-critical items are managed through strategies such as pooling purchasing requirements or adopting individual ordering systems to reduce administrative costs. These strategies seek to decrease the logistical and administrative complexity related to these items in order to optimize purchasing procedures and improve efficiency. Hajmohammad and Vachon (2016) suggest to re-evaluate the current purchasing strategy and gradually eliminate suppliers that are considered to pose a higher sustainability risk. (Caniëls & Gelderman, 2005; Hajmohammad & Vachon, 2016)

However, there are also critics of Kraljic matrix. Montgomery et al. (2018) state as the model is used qualitatively it may be one of its main flaws. According to the author, the

subjective evaluation of the suppliers or items in the matrix is heightened by the qualitative aspect. According to Goudarzi et al. (2023), contracts that take behavioural aspects into consideration are expected to have the greatest impact on strategic and bottleneck items. That is due to the buyer's relatively small supplier portfolio. Additionally, it has been argued by for example Keith et al., (2016) that the Kraljic Matrix's weakness is that it ignores a new novel form of power: the influence of extremely strategic and cooperative supplier relationships. (Montgomery et al., 2018; Goudarzi et al., 2023; Keith et al., 2016 in Balbi, 2019).

It can be stated that Kraljic matrix classifies products and suppliers in a simple four-category format. Nonetheless, as highlighted in this study, one of its main benefits is that it can evaluate risk associated with various product categories relatively quickly as a part of an interview. In other words, the Kraljic matrix was also used as a research tool for this thesis. After the literature review, the next chapter explores the research methods of design science research. The following chapter will provide a detailed explanation of this method, which forms the basis of the study.

3 Research Method

The selected research method for this master's thesis is design science research (DSR). According to Venable and Baskerville (2012, p.142) and Dresch et al., (2015) design science research can be used for inventing new artefacts. As said by Teperi et al. (2021) in DSR the created artefacts aim to be used for problem-solving methods for specific challenges that are often ill-defined or not fully understood by the general audience. The created artefacts can be for instance products, services and guidelines. Offermann et al. (2010) in Johannesson and Perjsons (p.31) have defined DSR artefact guidelines as "suggestions regarding behaviour in a particular situation." (Venable & Baskerville, 2012, p.142; Dresch et al., 2015; Teperi et al., 2021; Offermann et al., 2010 in Johannesson and Perjsons, 2014, p.31).

Since no specific guidelines for electricity distribution operators to comply with NIS2 supply chain management requirements existed prior to this study, design science was deemed the most suitable method for achieving this objective. The framework for design science research method in this thesis was primarily built using the book on design science research by Johannesson and Perjsons (2014) and the academic writing guideline book written by Hirsjärvi et al. (2009). These works along with supporting articles provided a theoretical background for developing the three-phase process of creating the guideline.

The supplier and product risk management levels are the two thematic levels that were the focus of the surveys and interviews for this thesis. While the supplier risk management level observes how DSO's manage risks at partner level the product risk level examines supplier risks through the lens of products as well as clarify the relationship between strategically important products and supplier risk. These two theme levels influenced the definition of the research questions and methodology.

3.1 Research process

The first phase of the DSR process in this study was done as an interview that contained both structured and semi-structured interview elements. As Johannesson and Perjons (2014) explain, a structured interview means sticking to a predefined protocol, consisting of a fixed list of questions. The responses are also predetermined, for example simply yes or no. In contrast, a semi-structured interview also follows a set of questions but they can be discussed in a flexible order. Semi-structured interview questions tend to be open-ended. Thus, they allow respondents to articulate their answers in their own words. The second and third phase of the process was done as a survey. According to Johannesson and Perjons (2014) the advantage of surveys is that they allow for collecting large amounts of data time-efficiently, but the disadvantage is that some individuals may choose not to participate at all, resulting in a low response rate. (Johannesson & Perjons, 2014)

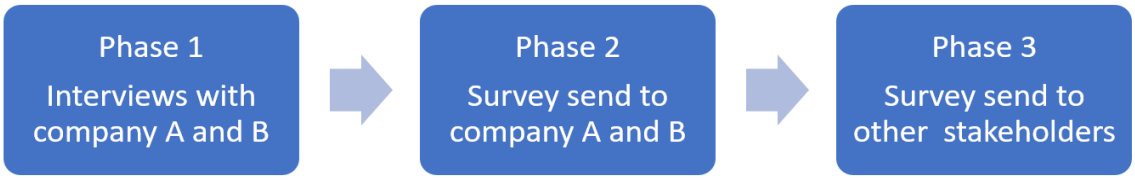

Figure 2. Phase one, phase two and phase three of the research process.

As illustrated in the picture above, the data gathered for the thesis was done in three phases. Phase one was carried out as two interviews in Teams with two different distribution system operators. These companies are referred to in this study as Company A and Company B. Phase two and three were executed as internet surveys. These surveys were identical to each other. Phase two involved the same companies as phase one. Phase three had a separate focus group.

3.2 Developing the guideline according to design science research methodology

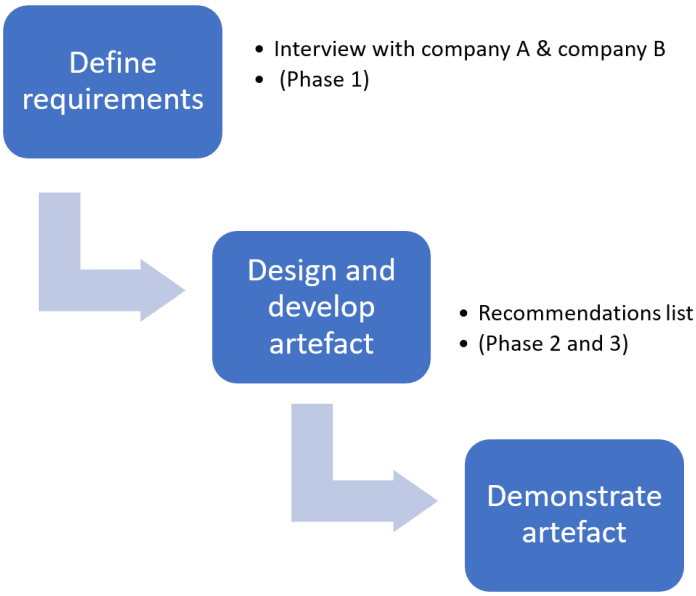

Figure 3. Developing the guideline artefact in accordance with Johannesson and Perjons (2014).

The picture above is describing the process of designing the guideline, alias the artefact, that was done according to Johannesson and Perjons (2014) example of design science method framework. While Johannesson and Perjons' (2014) method includes five steps, beginning with problem explication and concluding with artefact evaluation, this study chose to focus on the three central stages of the process. According to Johannesson and

Perjons (2014) this approach is common as many requirements- and development-focused design science research projects combine requirements definition with the actual artefact development. In this case, the need for the guideline was identified earlier during discussions between the researcher and DSO stakeholder groups. That served as an inspirational basis for the whole thesis. The final artefact was created after analysing survey results and identifying a gap. Following that, a lightweight evaluation of the artefact was conducted with the research group the thesis author was part of. (Johannesson & Perjons, 2014)

3.2.1 Phase one of the research process

In phase one the interviews with both company A and B followed the same structure. Interview group one, company A, had 8 participants, and group 2, company B, two participants. The meetings were agreed to be anonymous. The demographic data of the participants was gathered with a form, and the session were recorded for qualitative data analysis. The first part of the interview was a semi-structured thematic interview that aimed at highlighting specific aspects related to the application of the NIS2 legislation. Although supplier level was the primary thematic level of the first section of the interview, some aspects related to product risk were also covered.

Table 2. Questions utilized in interviews during phase one.

Research methodology	Thematic level	Theme	Question	Data analysis	Sub-chapter in the Results-chapter

Qualitative: Semi-structured interview	Supplier level	The overall responsibility of NIS2 implementation in electricity distribution companies in Finland	Who bears the responsibility for NIS2 implementation in the company?	Qualitative: Thematic	4.1.1.
Qualitative: Semi-structured interview	Supplier level	Supplier risk management	What are the possible cybersecurity risks from the vendors part that could affect you?	Qualitative: Thematic	4.1.3.
Qualitative: Semi-structured interview	Supplier level	Supplier risk management	What are the possible risks associated with outsourcing?	Qualitative: Thematic	4.1.3.
Qualitative: Semi-structured interview	Supplier level	Supplier risk management	When you conduct a risk assessment of a supplier, do you separately consider the risk of each supplier? Is the process then of varying scope depending on the supplier's risk level?	Qualitative: Thematic	4.1.3.
Qualitative: Semi-structured interview	Supplier level	Supplier risk management	Is it typical for a distribution network company to have suppliers from abroad, from EU countries, or entirely from outside the EU? Are risk classifications different for such operators?	Qualitative: Thematic	4.1.3.

Qualitative: Semi-structured interview	Supplier level	Standards and certificates of cybersecurity management	Do you currently hold an ISO 27001 certification, or are you planning to obtain one? Why yes or why not?	Qualitative: Thematic	4.1.2.
Qualitative: Semi-structured interview	Supplier level	Standards and certificates of cybersecurity management	Might the ISO 27001 standard become a requisite that you will formally expect from suppliers moving forward? Could it serve as a determining criterion in the selection of suppliers?	Qualitative: Thematic	4.1.2.
Qualitative: Semi-structured interview	Supplier level	Contracts and administration regarding cybersecurity	Are there any provisions written into the contracts in case a risk scenario occurs?	Qualitative: Thematic	4.1.4.
Qualitative: Semi-structured interview	Supplier level	Contracts and administration regarding cybersecurity	How do you consider in contracts if the ownership of the first vendor changes to a different country outside the EU?	Qualitative: Thematic	4.1.4.

All of the main questions from the first section of phase one are divided into the table above. The open-ended questions focused on the overall responsibility for NIS2 implementation in electricity distribution companies in Finland, standards and certificates of cybersecurity, supplier risk management and contracts and administration regarding cybersecurity. These topics were explored to determine the current level of supply chain cybersecurity management among electricity distribution operators and to identify key areas of importance and focus for the development of the final artefact, i.e. the guideline.

Although the interview topics were predefined, the phrasing of the questions varied as the interviews progressed.

Table 3. Information technology products, operational technology products and internet of things related products procured for electricity distribution operations.

Information technology (IT)	Operational technology (OT)	Internet of Things (IoT)
ERP CRM Cybersecurity Cloud computing Storage	SCADA DMS EMS Grid automation	Smart meter

The table above showcases the next part of phase 1. After the semi-structured interview, phase one transitioned into a structured interview. Initially, the groups were presented with a list of IT and OT products deemed strategically important to the DSOs, which was displayed in a PowerPoint slideshow. The existing literature and the researchers' understanding of the subject from discussions with stakeholders in the energy sector were the main sources of information for compiling this product list. The participants were requested to review the list and suggest additions or deletions of products based on their own knowledge. The table presented showcases in a simple manner that in which categories products and systems that are used in electricity sector and especially in distribution system operations can be categorized. The categorization follows the current axiom where these systems still operate as separate systems. In the left is information technology (IT), in the middle operational technology (OT) and in the right internet of things. The following chapters however focus more on IT and OT.

Table 4. Phase one second section of structured interview.

Research methodology	Thematic level	Theme	Question	Data analysis	Subchapter in the Results-chapter
Qualitative: Structured interview	Product level	Products strategic importance in relation to each other	Assessing products with Kraljic matrix	Qualitative data-analysis	4.2.
Qualitative: Structured interview	Product level	Connection of strategically important products to suppliers' risk	Assessing products with Kraljic matrix	Qualitative data-analysis	4.2.

The second table displays the questions related to the Kraljic matrix on a thematic level. Since the theme level shifts from supplier level to product level, it differs from the first section of phase one. Following that, the participants were then asked to place these products to the Kraljic Matrix based on how strategically important each product is to the DSOs. After gathering the interview data, the transcriptions were analysed and utilized for research phases two and three, that combined both legislative requirements as well as needs that emerged from the interviews.

3.2.2 Phase two and three of the research process

Phase two and three were carried out as surveys. These surveys were identical to each other. Phase 2 was conducted with the same interview group (company A and B). There were two respondents to the survey. Phase three had a different focus group, consisting of experts of academia, IT-industry as well as lawyers. Phase three was enforced to get a different perspective to the discussion from a focus group that works in the supply chain or stakeholder group with DSO's with the NIS2 themes. In the survey questionnaire, the format and order of the questions and statements were strictly predetermined. The surveys included multiple-choice questions based on NIS2 recital (85) and themes that

emerged from the first phase of the study. The aim was to identify the gap in DSOs' management of supplier relationships, both in terms of the requirements set by NIS2 and factors outside its scope that had emerged from the thematic analysis of the interview data.

Table 5. Phase two and three.

Research methodology	**Thematic level**	**Theme**	**Question**	**Data analysis**	**Subchapter in the Results-chapter**
Quantitative: Survey	Supplier and product level	NIS2 Recital (85) compliance	NIS2 Recital (85) compliance	Quantitative	4.3.1.
Quantitative: Survey	Supplier and product level	Compliance with recommended measures	Compliance with recommended measures	Quantitative	4.3.2.

The survey had four question sets. The first two question were to assess first the easiest and second the hardest measure of the same options to execute in order to comply with NIS2 requirements of supply chain and supplier management. These were derived straight from NIS2 Recital (85). The options were

1. listing all suppliers and subcontractors that have an effect on the cybersecurity
2. making a risk management model according to the list with an all-hazard approach and assess suppliers through the model
3. assessing and considering the suppliers or service providers cybersecurity practices
4. set and document requirements for cybersecurity in contracts
5. considering cybersecurity risks of complete supply chain
6. an open-ended question, asking whether the respondents would consider another mandated measure.

The last two questions were also to assess first the easiest and second the hardest measure of a list that was derived from the interviews, described as recommended measures

outside the mandated compliance to comply with NIS2 requirements of supply chain and supplier management. The options were

1. cooperating with stakeholders
2. focusing on component level security in supply chain risk management
3. considering legacy technology contracts, especially related to strategic items that in this case are operational technology
4. an open-ended question, asking whether the respondents would consider another non-mandated measure

Survey questions were asked in order to assess the gap the DSO's have in complying both with the mandated measures of NIS2 as well as the non-mandated measures.

3.3 Data analysis

Hirsjärvi et al. (2009) suggest that empirical data can be analysed after initial pre-work, which in this case involved transcribing the interviews following phase one and then reviewing the content. This suggestion was followed in the process of data analysis. The recorded interviews were transcribed and the read thoroughly. The data was analysed both qualitatively and quantitatively. It must be stated that in the research process, the qualitative analysis of phase 1 interviews played an important role in shaping the questionnaires of phase 2 and phase 3 that were later analysed quantitatively. After reviewing the material, the data was categorized by using thematic analysis. The thematic analysis followed the steps defined by Braun and Clarke (2021). Braun and Clarke (2021) define thematic analysis as a method for identifying, examining, and unravelling trends in qualitative data. It entails methodical data coding procedures which are used for creating themes. These themes serve as the primary analytic focus. (Hirsjärvi et al., 2009; Braun & Clarke, 2021)

The thematic analysis process, as outlined by Braun and Clarke (2021), consists of six steps: "(1) familiarizing oneself with the dataset", "(2) coding", "(3) generating initial themes", "(4) developing and reviewing themes", "(5) refining, defining, and naming

themes", and "(6) writing up" (Braun & Clarke, 2021). When working with the transcribed data, the preliminary work described by Hirsjärvi et al. (2009) effectively corresponded to step one of Braun and Clarke's method, as each transcribed line needed to be carefully reviewed. Once familiarization was complete, the data was coded by identifying segments that were relevant to developing the guideline. These segments are discussed in the next chapter of the thesis, where the results are presented. In step three, shared patterned meanings across the dataset were identified and generated as initial themes, which were first organized in an Excel file and later transferred back into text format. These themes were reviewed and named, they are visible as subchapters in the next chapter: 4.1.1 The overall responsibility of NIS2 implementation in electricity distribution companies in Finland; 4.1.2 Certificates of cybersecurity management; 4.1.3 Supplier risk management and 4.1.4 Contracts and administration regarding cybersecurity. (Hirsjärvi et al., 2009; Braun & Clarke, 2021)

Phases 2 and 3 of the study were executed via a survey format that is a form of structured interview also according to Hirsjärvi et al (2009). According to the writers, in a survey, the form and order of presentation of the questions and statements is completely determined. The quantitative data was collected from surveys conducted during phases 2 and 3. Statistical analysis was performed to identify which factors were perceived as the easiest and most challenging to comply with. Hirsjärvi et al. (2009) write that this format of data analysis is structured. However, the final section of the surveys included open-ended questions to capture perspectives that the author might not have anticipated, and are half-structured by nature. (Hirsjärvi et al., 2009).

The next chapter presents the results of the design science research process phase 1, phase 2 and phase 3.

4 Results

The results of the chosen research methods, interviews and surveys, related to phases 1, 2, and 3 covered in the previous chapter are presented in this chapter. Mirroring the literature review, the interviews and surveys addressed the two thematic levels explored in this thesis, namely supplier risk management and product risk management. Supplier risk management level aims to uncover the methods DSO's use to manage risks at the partner level. Product risk level examines supplier relationships through the lens of products. The objective was to clarify the relationship between strategically important products and supplier risk.

The two companies that participated in phase 1 and phase 2 were both DSO's of different regions in Finland. Both of these companies are large companies according to NIS2. Phase 3 had a more heterogenous participation population. The phase three targeted industry experts working as stakeholders for DSOs. These experts worked in academia, in the IT sector as well as lawyers.

4.1 Phase one semi-structured thematic interview results

As stated in chapter three, phase one was done as an interview with company A and B. The first part of the interview was done as a semi-structured interview. The second part was a structured interview. The themes discussed in the semi-structured interview were pre-determined with open-ended questions and open questions. The aim was to map the risks and means of cybersecure supply chain management in the electricity field. Three things that especially formatted phase 2 and 3 were three means to comply with NIS2 requirements. These were

1. cooperating with stakeholders
2. focusing on component level security in supply chain risk management
3. considering legacy technology contracts, especially related to strategic items that in this case are operational technology

Nevertheless, the discussions also gave rise to other topics, for instance who bears the responsibility of NIS2 implementation in DSO's operations, standards and certificates of cybersecurity management, cybersecurity related contracts and administration, and supplier risk management. Some of these topics are covered in NIS2 Recital (85).

The creation of the guidelines was impacted by phase one interviews, which, among other things, revealed and deepened information that would not have been understood from literature. This gave the guidelines a better understanding and direction for what areas to focus on when addressing supplier risk and product risk as well as complying with NIS2 requirements.

4.1.1 The overall responsibility of NIS2 implementation in electricity distribution companies in Finland

The interviews of phase one begun by exploring who bears the responsibility for NIS2 implementation in the distribution system operator organizations. The interviews revealed that, despite the Finnish Electricity Market Act (386/1995) requiring the separation of DSO operations from other electrical businesses, DSOs still tend to operate within larger corporate groups. Both the company A and company B interview included people who worked for the electricity distribution company as well as the local energy network provider. It became evident that DSO's in Finland tend to purchase information security and management services from the local energy network provider company. Cybersecurity services were part of these.

It was stated that DSO's carry a responsibility for their own company even though the cybersecurity services were acquired from the group company. The responsibility of implementing NIS2 on a company level was agreed to be a task of the management by both companies. However, company A separately emphasized that the organization aims to reach the compliance requirements by obtaining an ISO27001 cybersecurity certificate. This would entail personnel dedicated to ensure that the process of getting certified goes

as smoothly as possible. Company B representatives assumed that the implementation would be carried out at group company level but they did not intend to acquire a certificate for themselves.

4.1.2 Standards and certificates of cybersecurity management

Standards of cybersecurity management are recommended as a tool to comply with NIS2 requirements by several companies. Especially ISO27001 is one standard that is a popular tool stated by for example Fransila (2024) in his thesis that addresses implementing NIS2 in a company in Finland. That is one of the reasons why it was chosen to be a theme that would be addressed during the interviews.

When the companies were asked about reasons why they would possibly obtain a ISO27001 certification, it sparked a conversation about the standards benefits and downsides. According to Company A, the updated NIS Directive and certifications like ISO27001 give their software suppliers the ability to see which technologies are being used in the extended supply chain. Company A claimed that in this way, they also receive "lenses to what is happening beyond the first vendor." However, company A also mentioned some difficulties that come with the certification. One scenario that might occur is that a supplier might have an ISO 27001 certificate, but it might turn out that the information security practice is only being implemented on paper.

Yet again, the companies had different views on whether they need the certificate themselves. When the companies A and B were asked whether they have or are planning to obtain an ISO27001 certificate, the responses were quite different. Company A was having the standardization process underway during the interview time in February 2024 and they justified that decision by saying that it was something that was advised by external consultants. Company A had been advised that by implementing into its operations the ISO 27001 standard the company would be able to fulfil a significant portion of the NIS2 requirements by applying the standard. Company B participant explained that the buyer (the DSO) doesn’t sell software, thus they don’t need the certificate.

Company B interviewee responded that they don’t hold an ISO27001 certification but their company's operating model “largely mirrors it.” Another interviewee from company B added that the certification has been considered but has not been undertaken since it has not been perceived as something that would provide a competitive edge in the market. In terms of cybersecurity certifications company B claimed that their role in the supply chain in this context is more of a buyer than a supplier given that they don’t produce or sell software.

Following this, the companies were questioned about whether they believed the standard would become a formal requirement for suppliers and could be used as a determining criterion when choosing partners. In company A one respondent estimates that perhaps in larger projects ISO27001 might become a requisite. Another respondent stated that ISO27001 or its equivalent will be required especially in the future. They added that ISO27001 is easy to demand since the scope of its implementation can be defined. However, they stated that the problem with the standard is that not all operators have the same scope. In other words, certification can also be obtained with a more limited scope of execution. During the interview with company B one interviewee claimed that regarding the requirement of ISO 27001 from suppliers they need to consider the risk-based assessment. This means that each supplier is assessed separately and not all of them require the same safety-measures. ISO27001 could be “quite a big requisite” if there's a smaller supplier, because it might be an impossible requirement for some. Therefore, requiring ISO27001 might limit the pool of possible suppliers. However, the other respondent added that when a larger player can more convincingly state that it operates within the framework of legislation, directives, and standards as the buyer it usually simplifies the procurement processes so much that it leads to favouring such operators.

4.1.3 Supplier risk management

Following the discussion of the certifications, topics related to supplier risk management were covered. The companies were questioned about the largest cybersecurity risks they

believed to be associated with the vendors of their supply chain. Both product and technology-oriented risks as well as risks related to cybersecurity culture and administration were discussed.

The interviews revealed that one major technology risk of the procurement of software products was component risk. The information security of components and the vulnerabilities of what the possible flaws could pose could compromise the entire system's security. Furthermore, the use of legacy software whether it was employed by buyers or suppliers was seen as a potential threat. Company B gave an example that one way how a supply chain threat might materialize could be through data breaches resulted from operational methods or the technology used.

One cultural or administrative issue of the supply chains that was covered multiple times was the level of risk that the buying organization bears regarding the transparency of the subcontractor supply chain. Both companies stated that the understanding of the first subcontracting tier is usually on a good level but as the supply chain extends to second-tier subcontractors and beyond the visibility into operations and practices decreases. Correspondingly the control of that becomes also more difficult. In the interview with company B, it was mentioned that one consideration when evaluating the suppliers from the angle of cybersecurity is the information security controls that the supplier claims to have could in reality differ from their corporate processes. Therefore, company B claimed that the buyer cannot be absolutely sure that the vendor fully implements all of their cybersecurity requirements. Another perceived risk was that they might not be able to guarantee that the vendor fully implements all of their cybersecurity requirements.

During the interviews, the companies were questioned about whether they consider the risk associated with each supplier separately when conducting a risk assessment. The purpose of the question was to learn whether the buyer organization conducts risk assessments for each supplier with a different scope. From the interviews it rose that the

companies consider in their risk assessments that the software provider and subcontractors meet required standards. The companies pay special attention to open-source-systems and components that are used to ensure that the do not come from unreliable sources.

According to the interviews, the ISO27001 standards seemed to go hand in hand with both companies' procurement processes. It was emphasized that for instance a software that is supplied by a third-party who is most likely selected through a public procurement competition. Company B also stated that they use a method mirroring the standard when choosing suppliers. "We have a system in which software's are assessed into certain categories, like whether they are business-critical and then less critical, but the risk assessment actions in that scale are quite similar. The business-critical information systems are under a bit more scrutiny", is what one respondent of company B stated.

4.1.4 Contracts and administration regarding cybersecurity

From the interviews it could be stated that contracts played a major role in risk management of both DSO's. The interviewed companies stated that they have clauses in case of risk scenarios coming into reality. Company A stated that they have clauses in case of risk scenarios coming into reality, that are agreed upon and defined during the procurement phase. These are considered in their DPA agreements. DPA agreements include the right to audit as well as compensation and the obligation to rectify. Company B stated also that there are fundamental clauses if a risk scenario occurs. The contracts are written to include NIS2 compliant actions, stating who reports to whom and what actions should be taken. However, the responsibility cannot be completely shifted to a supplier by the client.

The companies' risk-management administrative measures took also account risks coming from suppliers that come abroad. Company A states that it is not typical to have suppliers from abroad, but it is important to consider that even if the supplier is local, the products and production components extend further. Therefore, it's possible that the contractual partner is a Finnish branch that is part of a group operating or having an ownership base elsewhere. Company B states that these cases are assessed thoroughly and holistically. However, they state that risk assessments of suppliers operating outside EU/EEA-region can be more difficult. One interviewee stated that "A good example is companies operating in the United States. Practically, the United States does not hand over any information about its companies, even to the authorities if you're doing any background checks."

Both companies emphasized that there are clauses that allow for the termination of the contract, since if for instance their partner is being bought by a company that operates outside EU/EEA, there happens information transfer outside EU and that is excluded by the contract. However, they note that there is a challenge if a physical component that includes AI that has long investment and holding times is procured, but the contract ends, they don't necessarily stop existing "out in the field".

4.2 Phase one structured interview results utilizing Kraljic matrix

The Kraljic procurement matrix, which was used in the structured interview happened in the second half of phase 1. However, the participants were required to look over a list of products prior to beginning the Kraljic matrix assignment.

Table 6. List of IT and OT products.

Information Technology products and systems	Operational Technology products and systems	Internet of Things
• ERP systems • CRM systems	• SCADA (Supervisory Control and	• Smart meters

• Cybersecurity solutions (firewalls etc.) • Data Analytics and Management Tools • Cloud Computing and Storage Services	Data Acquisition) Systems • Distribution Management Systems (DMS) • Energy Management Systems (EMS) • Grid Automation Equipment • Substation Automation Systems	

The product list that was given to companies A and B is replicated in the above table. First, companies A and B were asked to review a list of information technology and operational technology products, and to suggest any additions or deletions. Company A proposed adding integration platforms and network information systems (NIS). Company B suggested adding telecommunications. After this part the interviewees were shown the Krajlic matrix with a PowerPoint presentation. Both companies were required to evaluate the listed products according to the Kraljic procurement matrix methodology.

Table 7. Krajlic matrix in phase 1.

Leverage items • IT products in general • ERP • CRM • cybersecurity solutions	Strategic items • OT products in general • SCADA • DMS • NIS • integration platforms
Non-critical items	Bottleneck items

• grid and substation automation systems • cloud computing systems • data analytics systems	• OT products can be also as bottle-neck items • smart meters

The Kraljic matrix classification of the products by the companies A and B is shown in the table above. The table aims to mimic how the Kraljic matrix is presented in literature. Categories are leverage, strategic, non-critical and bottleneck.

Strategic items are presented in the upper right corner. Company A categorized SCADA, DMS, NIS and integration platforms as strategic items. Additionally, they included smart meters, noting the challenge that, despite the availability of multiple suppliers, integrating these into the overall system presents significant difficulties. This is because not all smart meters are interchangeable or easily integrated into the existing system. Company B, on the other hand, classified all operational technology products as strategic items.

Leverage items are in the upper left corner. Company A listed CRM, ERP, and cybersecurity solutions as leverage items, noting that while these are essential, their integration is complex and changing them is not straightforward. Company B indicated that all IT products would be categorized under leverage items.

Bottleneck items are presented in the lower right corner. Company B identified all operational technology (OT) products as bottleneck items. The interviewee emphasized the limited number of suppliers in the industry, which can make these products particularly vulnerable to becoming bottlenecks, especially in volatile global con-texts. They noted that the long lifespan and security requirements of these products often contribute to their scarcity. Furthermore, they pointed out that strategic products might overlap with bottleneck items and can swiftly transition between these categories. The interviews also discussed smart meters belonging to bottleneck items. Non-critical items are in the

lower left corner. Both company A and B classified grid automation, substation automation, cloud computing, and data analytics as non-critical items.

4.3 Phase two and three survey results

Phase two and three were carried out as surveys. These surveys were identical to each other. Phase 2 was conducted with the same interview group (company A and B). There were two respondents to the survey. Phase three had a different focus group, consisting of experts of academia, IT-industry as well as lawyers. Phase three was enforced to get a different perspective to the discussion from a focus group that works in the supply chain or stakeholder group with DSO's with the NIS2 themes. In the survey questionnaire, the format and order of the questions and statements were strictly predetermined. The surveys included multiple-choice questions based on NIS2 recital (85) and themes that emerged from the first phase of the study. The aim was to identify the gap in DSOs' management of supplier relationships, both in terms of the requirements set by NIS2 and factors outside its scope that had emerged from the thematic analysis of the interview data.

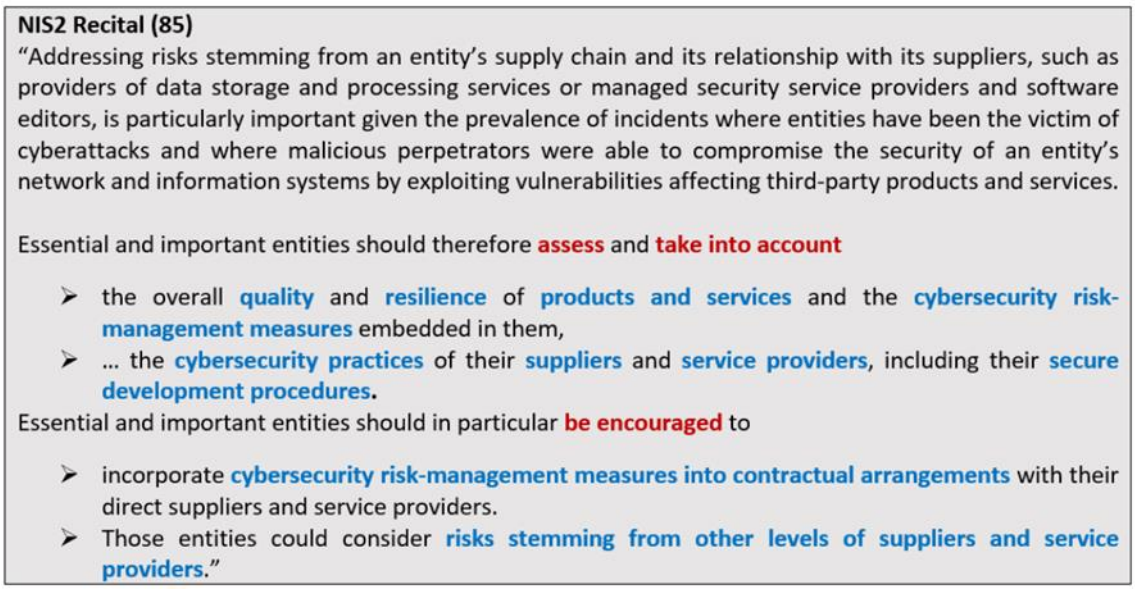

Figure 4. NIS2 Recital (85).

The first two multiple questions were about NIS2 recital (85) that is quoted directly in the picture above. The options were formed with the recommendations given by Traficom (2024) and FISC (2024). The picture was also shown with the survey. The first question was asking “which measure do you consider the easiest in order to comply with NIS2 requirements of supply chain and supplier management” whereas the second asked the “most challenging” measure. Options were

1. Listing all suppliers and subcontractors that have an effect on the cybersecurity
2. Making a risk management model according to the list with an all-hazard approach and assessing suppliers through the model
3. Assessing and considering the suppliers service providers cybersecurity practices
4. Set and document requirements for cybersecurity in contracts
5. Considering cybersecurity risks of complete supply chain
6. An open-ended question, asking whether the respondent would consider another mandated measure

The third and fourth multiple questions were derived from the interviews conducted in phase one. The third question was “which one of the recommended measures outside the mandated compliance do you consider easiest to comply with” and fourth one asked about the most challenging one to comply with. The options were

1. cooperating with stakeholders
2. focusing on component level security in supply chain risk management
3. considering legacy technology contracts, especially related to strategic items that in this case are operational technology
4. an open-ended question, asking whether the respondents would consider another non-mandated measure

4.3.1 Phase two survey results

As stated before, phase two involved the same companies referred to as company A and B which were also interviewed in phase one. Primary goal of phase two was to identify

the gaps that distribution system operators have in their management of supplier relationships, both in terms of NIS2-mandated requirements and external factors that surfaced from the interview data's thematic analysis.

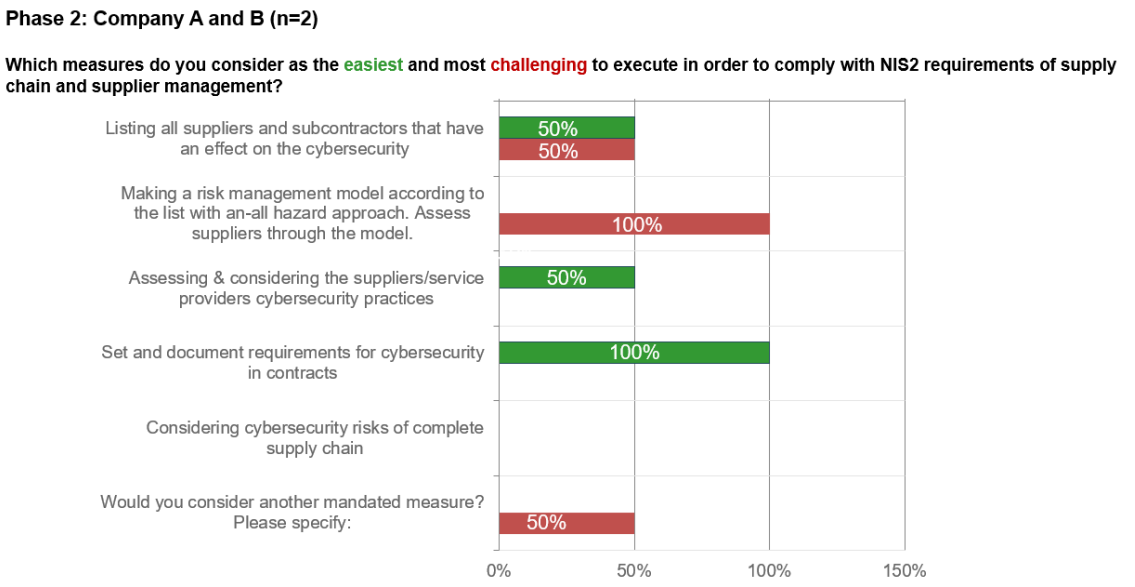

Figure 5. Phase two multiple question one and two.

The image above combines the answers to the first two questions. The first two multiple questions were about NIS2 recital (85). The first question was asking “which measure do you consider the easiest in order to comply with NIS2 requirements of supply chain and supplier management”. However, as the questionnaire was multiple choice, the actual evaluation of which measure would be considered easiest or hardest per se is impossible to evaluate. Phase two companies evaluated “listing all suppliers and subcontractors that have an effect on the cybersecurity” (50% of respondents), “assessing and considering the suppliers/service providers cybersecurity practices” (50% of respondents) and “setting and documenting requirements for cybersecurity in contracts” (100% of respondents) to be the easy methods to comply with the mandatory requirements of NIS2. The hardest of mandatory requirements of NIS2 to comply with were seen to be “listing

all suppliers and subcontractors that have an effect on the cybersecurity" (50% of respondents) and "making a risk management model according to the list with an-all hazard approach" (100% of respondents). Furthermore, it was stressed that taking the entire supply chain into account will be the most difficult measure in phase 2's open section "would you consider another mandated measure" (50% of respondents).

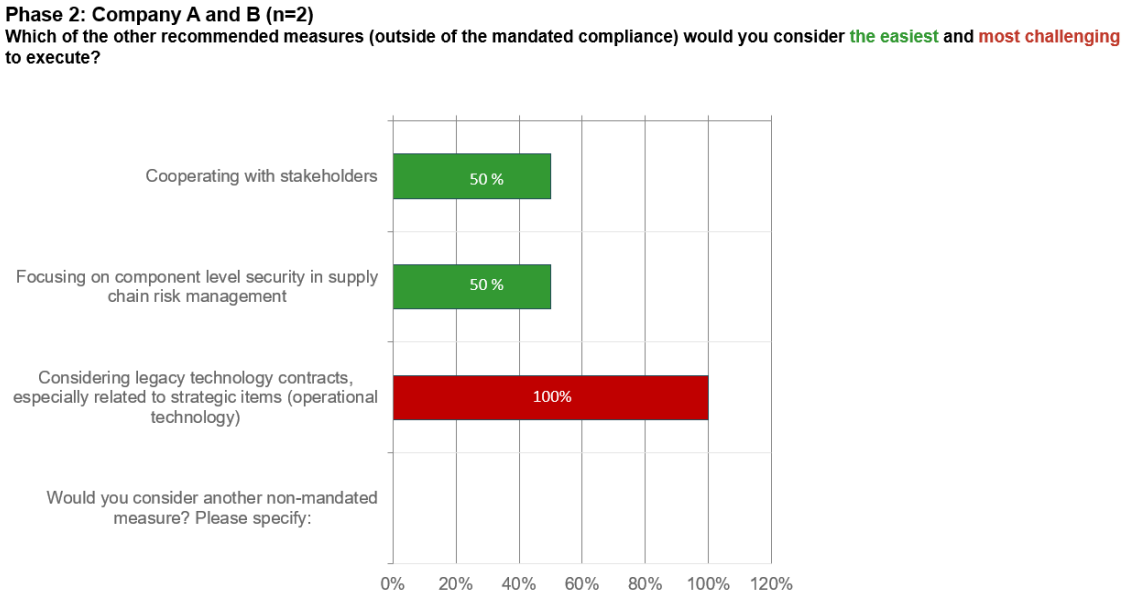

Figure 6. Phase two multiple question three and four.

On the image above are displayed what the respondents ought to be the easiest and most challenging measure outside the mandated compliance. The situation is similar as in the first two questions; the questionnaire was multiple choice and thus the actual evaluation of which measure would be considered easiest or hardest cannot be evaluated directly. Of the other recommended measures outside of the mandated compliance considered easiest to execute was "cooperating with the stakeholders" (50%) and "focusing on component level security in supply chain risk management" (50%). The most challenging was considered to be "considering legacy technology contracts, especially related to strategic items (operational technology)" (100% of the respondents).

4.3.2 Phase three survey results

Phase three had a different focus group, consisting of experts of academia, IT-industry as well as lawyers. Phase three had the same questions as phase two. The questionnaires were also multiple choice, and thus the answers reflect generally which measures are considered either easy or challenging. The respondents were asked assess the questions from the perspective of distribution system operators. The aim was also to find out the gap that distribution system operators have in their management of supplier relationships, both in terms of NIS2-mandated requirements and external factors that surfaced from the interview data's thematic analysis but with a different angle. The angle in the case of phase three was to obtain outsider perspective on what the gap could be.

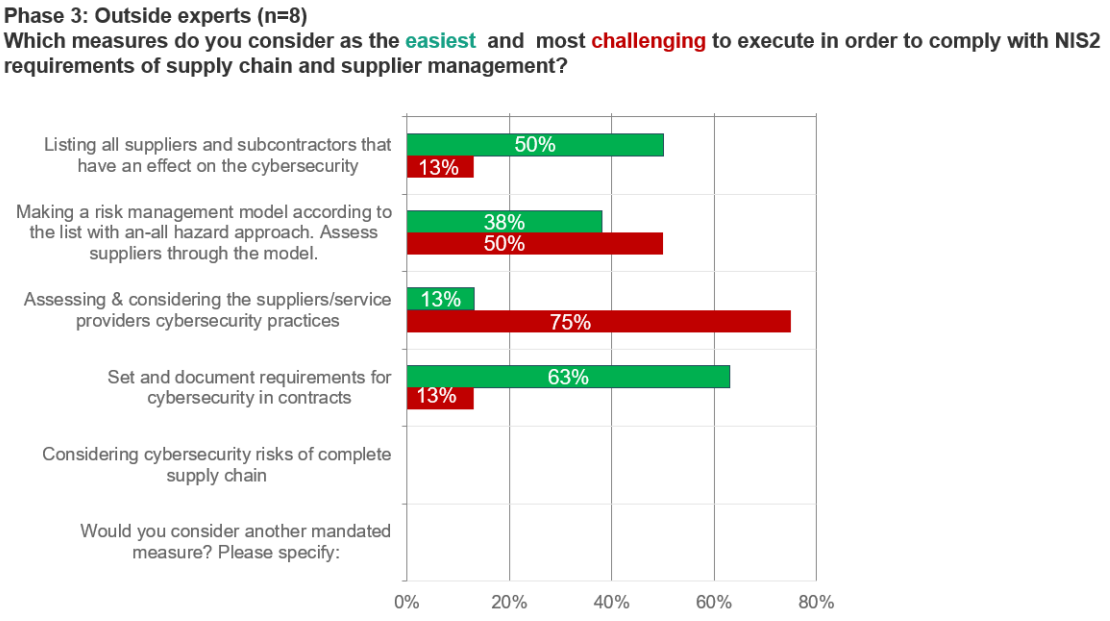

Figure 7. Phase three multiple questions one and two.

The above picture showcases phase three question one and question two results. Phase three respondents assessed as easiest measures to comply with NIS2 requirements “listing all suppliers and subcontractors that have an effect on the cybersecurity” (50% of respondents) although 13% of respondents considered this as a hard measure to comply with. Also, “making a risk management model according to that list with an-all hazard

approach and assessing suppliers through the model" was seen easy (38% of respondents) even though majority of the respondents considered it hard (50%). The highest amount of people considered easy "setting and documenting requirements for cybersecurity in contracts was seen the easiest to be done" (63% of respondents) and a small percentage considered it hard to comply with (13%). The most challenging measure was seen to be "assessing & considering the suppliers/service providers cybersecurity practices" (75% of respondents) but a percentage of 13 of the respondents considered that measure easy.

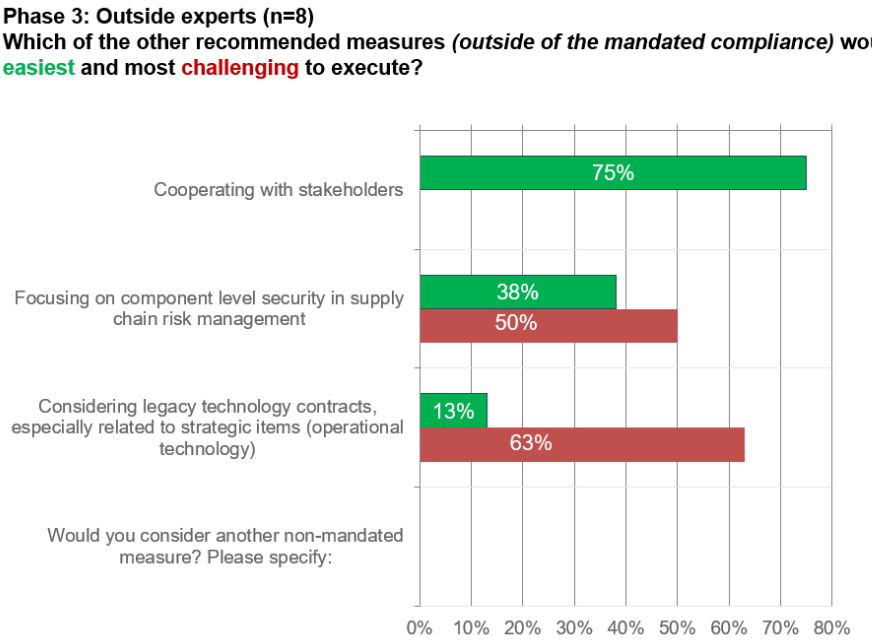

Figure 8. Phase three multiple questions three and four.

The above picture showcases phase three question three and question four results. When assessing the recommended measures outside of the mandated compliance, the easiest to execute were seen to be "cooperating with stakeholders" (75% of respondents) and next "focusing on component level security in supply chain risk management" (38% of respondents). The most challenging measure outside of the mandated compliance was seen to be "focusing on component level security in supply chain risk management" (50% of respondents) and "considering legacy technology contracts, especially related to strategic items (operational technology)" (63% of respondents).

5 Discussion

The aim of the discussion chapter is to provide an overview to the thesis work. This thesis explores different methods for cybersecurity management through two central themes. These themes are a supplier risk management and product risk management. The thesis uses design science research as a method for formulating an artefact that is aimed to work as a guideline. The guideline is created for complying with NIS2 supply chain requirements and considers also other aspects of cybersecurity. The target group for the work is the is electricity distribution system operators in Finland. The lack of a guideline specifically designed for this target group prior to the beginning of thesis work was the catalyst for creating one. Before this chapter presents the aforementioned guideline, the discussion assesses the chosen research methods and challenges while conducting this research. Secondly, the chapter moves to the thematic categories through which the literature and research method results are compared. Thirdly, the chapter presents the guideline that is formulated after all this.

5.1 Research methods

The chosen research method for this thesis was design science research. Design science research can be used to create new artefacts, according to e.g. Venable and Baskerville (2012, p. 142) and Dresch et al. (2015). Teperi et al. (2021) contend that in DSR, the created artefacts, such as guidelines, aim to be used for problem-solving methods for specific challenges that are often ill-defined or not yet completely understood by the general audience. Since no specific guidelines for electricity distribution system operators on how to comply with NIS2 supply chain requirements existed prior to this study, the thesis work aims to do that as well as provide insights on what they should consider from both product and supplier cyber risk. This decision is also justified by the results of the thesis by Linderoth (2024) where it is stated that maintaining supply chain compliance with NIS 2 is the most significant challenge the energy sector will face. Additional recommendations outside the mandated scope of the legislation are given too. Due to

the nature of the work, design science was determined to be the most appropriate approach for developing the guideline. The surveys and interviews conducted for this thesis focused on the two thematic levels: supplier and product risk management. The product risk level looks at supplier risks from the perspective of products and explains the connection between supplier risk and strategically significant products, whereas the supplier risk management level monitors how DSOs manage risks at the partner level. The way the research questions and methodology were defined was impacted by these two theme levels. The research process itself was conducted in three phases. (Venable & Baskerville, 2012, p.142; Dresch et al., 2015; Teperi et al., 2021)

5.1.1 Research process

Phase one was done as an interview with company A and B that both were distribution system operator representatives. The first part of the interview was done as a semi-structured interview. The questions were formed through discussions with energy sector stakeholders, literature review and discussions with the research group the thesis writer worked in at the time the thesis has been written. The themes discussed in the semi-structured interview were pre-determined with open-ended questions and open questions. The aim was to map the risks and means of cybersecure supply chain management in the electricity operations field. The second part of phase one was a structured interview that utilized Kraljic matrix. The aim was to find out how strategically important different IT/OT products are in relation to each other as well as the connection of strategically important products to suppliers' risk. Phase two and three were conducted as surveys to different target groups. The survey questions were formed both through the literature review and from the analysis of phase one interviews. The two companies that participated in phase 1 and phase 2 were both DSO’s of different regions in Finland. Both of these companies are large companies according to NIS2. Phase 3 had a more heterogenous participation population. The phase three targeted industry experts working as stakeholders for DSOs. These experts worked in academia, in the IT sector as well as

lawyers. Phase three's goal was to identify the gaps in DSOs' supplier relationship management, both in terms of NIS2-mandated requirements and additional aspects that surfaced from the interview data's thematic analysis.

5.1.2 Analyzing the data

The data was gathered for the thesis with interviews and surveys. The interviews started out with a semi-structured part that as Johannesson and Perjons (2014) explain, follows a set of questions but they can be discussed in a flexible order (Johannesson & Perjons, 2014). Semi-structured interview questions tend to be open-ended. Thus, they allow respondents to articulate their answers in their own words. This gave a chance to do a thematic analysis as well as get a broader overview on the topic of the research. One of the limitations noticed during the interviews was some of the interviewees gave answers that were "off-topic" from the questions' intended focus. Also, because of the time constraints during the interviews, it was sometimes a must to move the conversation along, that unfortunately hindered the chance thoroughly examine the perspectives of every participant. When the interviews of phase one progressed to the structured part the setting was simpler in a sense. It was possible to stick to a predefined protocol that was categorizing the products to the Kraljic matrix. However, it didn’t give the same opportunity to ask questions that can give answers that go a bit deeper under the surface as the semi-structured interview did.

Phase two and three were conducted as surveys. According to Johannesson and Perjons (2014) the advantage of surveys is that they allow for collecting large amounts of data time-efficiently, but the disadvantage is that some individuals may choose not to participate at all, resulting in a low response rate (Johannesson & Perjons, 2014). One significant issue, particularly during phase three, was indeed the low response rate of two respondents. The reason behind this might be because surveys can be boring to answer or the recipient people get so much email that the message will go unnoticed.

However, phase three was partly conducted due to the matter of phase two having such a low response rate.

The core aim of the thesis is to form a guideline for NIS2 compliance and general aspects for electricity distribution system operators to consider about cybersecurity. As this can be looked from two aspects, namely product and supplier risk management, the discussion will follow that categorization.

5.2 Assessing the product and supplier risk aspects of the revised Network and Information Security Directive

According to the European Commission (2023), the Network and Information Security Directive is being revised so that European Economic Area is able to meet the growing cybersecurity needs. This revision (NIS2) includes for instance new reporting prerequisites and a size-threshold rule. The list of entities covered in the directive has grown. Additionally, new cyber risk management aspects such as the supply chain risk management are introduced in the revised directive. In NIS2 the both the recital (85) and article 21 part (d) and (e) are considered specifically relevant for this thesis. These introduce the supply chain management aspect of the directive. The recital (85) addresses supply chain and supplier relationship cyber-risk, particularly posed by third-party suppliers. Article 21 point (d) and (e) look at both the suppliers and products. As point (d) measure is "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers" it can be seen to relate directly to how essential it is to safeguard and manage the relationships that the organization has with the vendors or service providers it depends on to sustain its operations. Therefore, this level of the legislation can be seen to be on a human oriented, security culture and administrative level, in line with this thesis. And point (e) measure "(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure" refers to that the entities should prioritize the cybersecurity aspects of product lifecycle management from procurement to

ongoing use. Therefore, this level of the legislation can be seen to be on a product oriented, technology risk, strategic choices level, in line with this thesis. (European Commission, 2023; Directive (EU) 2022/2555)

This thesis has been examining the recommendations for NIS2 published by FISC (204) and Traficom (2024) while the work was already started. However, while conducting the literature review part, there were still not many academic references about the topic. The reason for this might be because this thesis was mostly written in early 2024, while the national transposition for the directive is in October 2024. While the recommendations by FISC and Traficom were analysed, points of alignment were noticed to recital (85). A summary of these recommendations and a chapter containing them are included in the literature review. According recital (85) the organizations referred to as entities "should" evaluate and consider "the resilience and quality of their products and services" as well as the cybersecurity risk-management strategies incorporated into these products and services. These entities “should” also evaluate the secure development procedures and cyber-security policies of their service providers and suppliers. They "could" also want to evaluate supply chain relationships and operational aspects like procurement and product lifecycle management and taking into consideration risks arising from different tiers of suppliers and service providers. There is a difference in requirements between the wording “should” that indicates that something is mandatory to do versus “could”. Traficom (2024) and FISC (2024) recommend listing all suppliers and subcontractors that have an effect on the cybersecurity as well as making a risk management model according to the list with an all-hazard approach and assessing the suppliers through the model. The authorities recommend assessing and considering the suppliers and service providers cybersecurity practices, setting and documenting requirements for cybersecurity in contracts. They also recommend considering cybersecurity risks of complete supply chain. The condensed version of recommendations given by Traficom and FISC were directly used for the research surveys question one and two utilized in phase two and three. (Directive (EU) 2022/2555; Traficom, 2024; FISC, 2024)

5.3 Phase 1 of the research process

5.3.1 The overall responsibility of NIS2 implementation in electricity distribution in Finland

The interviews looked first at the overall responsibility of NIS2 implementation in electricity distribution companies in Finland. Distribution system operators are defined as a part of the electricity sector, defined as essential entities in NIS2. These entities are subject to especially strict compliance requirements. It has been recognized by for instance by the Finnish National Emergency Supply Agency (2022) that the energy sector is divided between entities with high and low maturity levels, and the cybersecurity culture varies among these entities. The electricity distribution operator companies vary of size too, so it can be estimated that the smaller DSO's might have different cyber maturity compared to the larger players. Additionally, it has been identified in Finland that organizations operating over larger geographical areas have invested more in cybersecurity compared to local entities. The companies (A and B) interviewed operate in separate geographical areas but both of them revealed to be large-size companies. The interviews didn't directly reveal the investment differences between the companies A and B. That is however given in terms of electricity distribution operators having a natural monopoly meaning that one geographical area has one operator. (Finnish National Emergency Supply Agency, 2022; Finnish Government, 2024; The Finnish Energy Authority 2022; Finnish Energy, 2024b)

The two DSO's that were interviewed belonged to the same group company as the local energy network provider even if the law requires them to be separated from each other. Notable from the NIS2 aspect was that it became evident the DSO's tend to purchase information security and management services, including cybersecurity, from the local energy network provider company. From a cybersecurity perspective, this could lead to an increase in risk exposure. Benaroch (2020), for instance, has argued that organizations that outsource their IT and cybersecurity responsibilities typically assume that the service providers will take on the responsibility for managing cybersecurity risks. In practice,

this may result in the risk profile growing in both organizations. However, it was emphasized that DSO's carry a responsibility for their own company even if the cybersecurity services were acquired from the group company. The responsibility of implementing NIS2 on a company level was agreed to be a task of the management by both companies. (Benaroch, 2020)

As NIS2 requires companies to enhance their cyber supply chain risk management (CRSM) that include different methods such as quality assessments, third-party auditing, utilizing and requiring standards in contracts and aligning interests and cooperating with stakeholders within the supply chain, the interviews focused on these and the thematic risk categories. (Boyson, 2014; Borenius et al., 2022)

5.3.2 Thematic categories of phase one

5.3.2.1 Supplier risk management in cybersecurity

According to the literature, cooperating with the stakeholders, sharing information, communication and other risk management things are considered important for supplier risk management. These actions might increase supply chain visibility, although for example standards do that as well as shown later. Here the idea was to see what risks stem for suppliers. One cultural or administrative issue of the supply chains that was covered multiple times was the level of risk that the buying organization bears regarding the transparency of the subcontractor supply chain. Both companies stated that the understanding of the first subcontracting tier is usually on a good level but as the supply chain extends to second-tier subcontractors and beyond the visibility into operations and practices decreases. according to Traficom (2024) the entity should choose risk management measures that fit the supply chain and execute the measures to those suppliers, in the situation when risk management measures have a cybersecurity-promoting effect. FISC (2024) recommends to use a basic model of information security as a reference framework for the evaluation. FISC (2024) also recommends to organize suppliers according to the risk level, the so-called risk category. The risk category consists of at least two aspects:

the importance of the supplier to the company's (or entity's) own operations and the avail-able information on the supplier's own risk management.

Company B also stated that they use a method mirroring the (ISO27001) standard when choosing suppliers. "We have a system in which software's are assessed into certain categories, like whether they are business-critical and then less critical, but the risk assessment actions in that scale are quite similar. The business-critical information systems are under a bit more scrutiny", is what one respondent of company B stated. There are different measures to be taken during the supplier life cycle according to for example Verlag (2013) and Boyson (2014). Pre-contract coordination efforts include incorporating clauses into vendor contracts that obligate vendors to address cyber risk. Mid-lifecycle, a formal agreement with the vendor outlines the execution of time-based mitigation steps. Compliance can be evaluated through a vendor rating system. Contracts and standards are seen important measures to reduce the supply chain cyber risk in academic literature as well as in the recommendations given by Traficom (2024) and FISC (2024), also addressed in the NIS2 Directive. (Directive (EU) 2022/2555; Traficom, 2024; FISC, 2024; Verlag, 2013; Boyson, 2014)

5.3.2.2 Contracts and administration regarding cybersecurity

From the interviews it could be stated that contracts played a major role in risk management of both DSO's. The interviewed companies stated that they have clauses in case of risk scenarios coming into reality. Contracts are seen as a key part of cybersecurity risk management in academic literature and Traficom (2024) and FISC (2024) have recommend to use contractual means in order for the buyer to be ensured about the procurement safety. These means can be requiring certifications, examining the product characteristics and by ensuring the reliability of the supplier and preparing for risks.

The companies' risk-management administrative measures considered risks coming from suppliers that come abroad. Traficom (2024) has outlined that the buyer should be

prepared in changes in the contracts they make. These changes could entail for example changes in ownership or changes regarding the service providers. It was stated in the interviews that it is not typical that the DSO's have suppliers from abroad. However, it was emphasized that even though the initial supplier, or vendor, is normally local, the products and production components go beyond that. Consequently, it is possible that the contractual partner is a Finnish branch of a company that operates or has ownership interests in other countries. It was mentioned that these cases are evaluated carefully and comprehensively. Nevertheless, it was also stated that it is more challenging to execute risk assessments to suppliers who operate outside of the EU/EEA region. According to the interviews, there are provisions in the contract that permit the contract to be terminated for example, if their partner is acquired by a business that is not based in the EU or EEA. This can be justified by the information that is then being transferred outside of the EU. This is usually excluded by the contract.

Traficom (2024) has advised that after a company has finished the supplier risk assessments, the cybersecurity requirements should be set in contracts. According to FISC (2024), a contract should not state directly that the supplier "must meet the requirements of the NIS2 directive" in order for assuring that the supplier complies with legal requirements. Interestingly, though, during the interviews, it was mentioned that NIS2 compliant actions, which specify "who reports to whom and what", are explicitly written into contracts. This statement may have been made because the interviewees were not legal experts, meaning that since they are probably not in charge of drafting the contracts, they may not know how contracts are formed in detail. Nevertheless, it was emphasized that even in cases where the client demands NIS2 or ISO 27001 compliance, the responsibility cannot be completely shifted to a supplier.

5.3.2.3 Standards and certificates of cybersecurity

The requirement of cybersecurity standards in the supply chain was discussed in the interviews. The interviews during phase one showed that both DSO's require some kind of

cybersecurity certifications from their suppliers. However, it was not agreed that they require specifically ISO27001 although it was estimated that perhaps in larger projects ISO27001 might become a requisite when choosing a supplier. For example, Kanstren et al. (2017) have argued that industry certifications like ISO27001 play an important role in defining cybersecurity requirements and managing suppliers and subcontractors with varying security practices. This is seen particularly relevant due to the current trend of organizations outsourcing their IT and cybersecurity services as end products are often built of chains of subcontractors and integrations of their subsystems leading to external dependencies in the supply chain. ISO27001 was seen as a barrier to ask from a smaller supplier because it might be an impossible requirement for some. Therefore, it was seen that requiring ISO27001 might limit the pool of possible suppliers. However, it was noted that larger suppliers can possibly show more clearly that they follow the cybersecurity requirements defined by legislation and standards. This was seen to simplify the procurement processes and estimated to making them more likely to be favoured.

It has been stated by Calder (2008) that certification builds trust with clients by demonstrating effective information security practices. Hamdani et al. (2021) have argued that if a supplier utilizes a standardized approach to risk management, it is easier for the buyer to assess its compliance. This became evident in the interviews too as the companies emphasized that both the upcoming legislation as well as certifications such as ISO27001 make the extended supply chain more transparent as the cybersecurity requirements are the known throughout the supply chain. However, a limitation was also mentioned with cybersecurity certifications, as was seen by the companies that the information security practice is only being implemented on paper.

Especially ISO27001 standard was deemed to be easy to demand as its scope of implementation can be defined. As Heras-Saizarbitoria and Boiral (2013) put it, standards establish the minimum acceptable level of performance or quality, as well as the optimal level an organization must meet to be considered compliant. However, in the interviews it was stated that the problem with the standard is that not all operators have the same

scope. In other words, certification can also be obtained with a more limited scope of execution. It was also stated that ISO27001 was required from companies after assessing whether they are so risky that they need to provide that certification or in what scope at least. Yet again, the companies had different views on whether they need the certificate themselves. Company A was informed that it could meet a significant portion of its NIS2 obligations by applying ISO 27001 framework into its operations. Company B stated that the DSO, alias the buyer in the case of cybersecurity, does not need the certification as they do not sell software. Thus, it was seen that obtaining the certification does not give the DSO's competitive advantage although it was stated that the way they operate closely resembles ISO 27001.

5.3.2.4 Product risk in cybersecurity

The interviews addressed the possible risks stemming from products in the supply chain. Software vulnerabilities and networked systems are seen as the two main product risks according e.g. Kumar and Mallipeddi (2022). Especially in the academic literature it seems to be an axiom that the electricity sector has specific cybersecurity issues related to legacy technology, that in the case of electricity distribution operators seems to be especially the operational technology products. The conventional more IT driven methods of managing cybersecurity risks are commonly seen not applicable to the sector. It was also anticipated that during the second part of phase two utilizing the Kraljic matrix that the interviewees would categorize OT and IT products differently, as it has been noted in the literature that the electricity sector is in a way dependent on the legacy technologies. Additionally, the threats related to product components has been recognized to be an issue in the energy sector. (U.S. National Institute of Standards and Technology, 2024; Borenius et al., 2022; Maleh, 2021)

The risks related to product components as a key technology risk associated with software procurement were highlighted in both interviews. It was acknowledged that the possible components' vulnerabilities could compromise the security of the whole product or system. Furthermore, the use of legacy software by both suppliers and buyers was

noted as a threat factor. An example given was that that data breaches brought on by legacy technology or outdated operational methods could materialize as cyber incidents in the supply chain. Both interviewed companies stressed the importance of carefully assessing the open-source systems and components to ensure they do not originate from unreliable sources. A method how to tackle the component security issue is addressed by for instance Traficom (2024) and FISC (2024) is that the supplier could request a component list of critical products and services (e.g. SBOM, software bill of materials or HWBOM, hardware bill of materials) if necessary to identify and manage dependencies and vulnerabilities against them. (Traficom, 2024; FISC, 2024)

During the interviews it was also noted that there is a challenge if a physical component that includes AI that has long investment and holding times is being procured. The challenges or risks stem when the contract ends, as these products can be planted to “out in the field” and they don’t necessarily “stop existing” even if their contract life cycle has ended. This is a product life-cycle management factor that the suppliers should consider when making the contracts with the suppliers.

5.3.3 Kraljic matrix in phase one

One method of assessing product and supplier risk was aimed to do with Kraljic matrix that took part also during phase one as a structured interview. According to for example Caniëls & Gelderman (2005) Kraljic matrix can be used as a tool to assess the strategic importance of different suppliers by categorizing products either as strategic, leverage, bottleneck or non-critical items (Caniëls & Gelderman, 2005). During this research the usage of the Kraljic matrix aimed to especially find out the strategic importance of different IT and OT products in relation to each other and the supplier as well as the connection of strategically important products to supplier risk.

As it has been acknowledged in the literature that electricity sector operators are in some ways dependent on legacy technology items that are often operational technology products, it was expected that the interviewed companies would categorize at least

partly OT products as strategic items. This expectation was confirmed, as company B categorized all operational technology products as strategic items albeit in a somewhat generalized manner. Also, company A categorized from OT products SCADA, DMS, NIS and integration platforms as strategic items. There was also a debate during the interview with company A whether smart meters, which are in this thesis included in the category of "Internet of Things (IoT) related products" belong in the bottleneck or strategic item categories. Company A pointed out that, even though there are several suppliers, integrating these into the system often presents a significant challenge. This categorization could be seen suggesting that these items could instead be categorized as bottleneck items. According to the National Audit Office of Finland (2023) reliance on a single supplier can be due to market conditions or procurement processes but generally this situation should be avoided (National Audit Office of Finland, 2023). However, in the interviews it was noted that there is a lack of OT suppliers in the market. Therefore, distribution system operators could benefit from forming strong alliances and collaborative risk management approaches with both OT product and system suppliers and smart meter suppliers as suggested by for instance Caniëls and Gelderman (2005) and Hajmohammad and Vachon (2016).

Company B continued the broad categorization with IT products, suggesting that all IT products and systems belong to the leverage item category. Company A listed CRM, ERP, and cybersecurity solutions as leverage items. Although classifying these products as leverage items, company A wanted to emphasize that they are not easily changed due to their complex integration. Therefore, it is probably not as suggestable to change the suppliers so often as it might be with different IT systems. It might be beneficial for the distribution system operators to develop strategic partnerships with technologically advanced suppliers to enhance competitive advantages as Caniëls & Gelderman (2005) suggest to do with leverage items. This strategy is confirmed also by Hajmohammad and Vachon (2016) who say that cooperative measures can be a better strategy to deal with leverage item suppliers as it helps maintain a larger pool of suppliers in the long term.

When the bottleneck items were discussed, company B claimed that OT products can also be bottleneck items. Thus, products and systems categorized as strategic can overlap with the bottleneck categorization. This was justified by an interviewee claiming that there is a lack of suppliers in the market making these products especially prone to becoming bottlenecks, especially in unpredictable global settings. Company B also had observed that as these products have long lifecycle and strict security requirements, it also adds to why the supplier pool is limited. Caniëls & Gelderman (2005) suggest that when dealing with bottleneck items, the purchasing organization accepts their dependence of these products and focus on mitigating the negative impact of a situation possibly deemed unfavourable. According to Kraljic's model Hajmohammad and Vachon (2016) recommend ensuring the supply for the bottleneck items even at higher prices. As Caniëls & Gelderman (2005) suggest, distribution system operators could aim to maintain some stock of smart meters if that is possible. Also, seeking to reduce dependence by finding other suppliers could be the case with smart meters. With OT products applying these strategies might not be possible. Therefore, it might be more beneficial to form strong alliances and collaborate with OT product suppliers as suggested to do with strategic items.

The emphasis on discussions about items considered non-critical was low during the interview, possibly as they are non-critical and the focus was specially to find out which items should be categorized as the strategic items. Both company A and B classified grid automation products, substation automation products, cloud computing products, and data analytics products as non-critical items. As the items in this category can be easily replaced, one strategy could be to save from this product category by pooling purchasing requirements as suggested by Caniëls & Gelderman (2005).

5.4 Gap analysis according to phase two and three

Phase one interviews had an impact creating the guidelines. The first phase of the research covered a number of subjects, such as supplier risk management, cybersecurity-

related contracts and administration, standards and certifications for cybersecurity management, and the responsibilities for NIS2 implementation within the distribution system operators. Furthermore, the relationship between supplier risk and strategically significant products was investigated, as was the strategic importance of different IT and OT products in relation to one another. Indirect discussion of a few of these subjects can be found in NIS2 Recital (85). However, as the recommendations by both Traficom (2024) and FISC (2024) that are often referred to in this thesis were published after the interviews, it was realized that a more structured gap analysis would be required. Therefore, a condensed format of the recommendations reflecting the recital (85) requirements was listed in phase two and three as measures of NIS2 compliance. They also formed the question one and question two. The first question was asking “which measure do you consider the easiest in order to comply with NIS2 requirements of supply chain and supplier management” whereas the second asked the “most challenging” measure.

1.Listing all suppliers and subcontractors that have an effect on the cybersecurity
2.Making a risk management model according to the list with an all-hazard approach and assessing suppliers through the model
3.Assessing and considering the suppliers service providers cybersecurity practices
4.Set and document requirements for cybersecurity in contracts
5.Considering cybersecurity risks of complete supply chain
6.An open-ended question, asking whether the respondent would consider another mandated measure

However, especially as the first part of the semi-structured interview had discussions that went beyond the topic of the thesis, they deepened the knowledge of electricity distribution operator specific cybersecurity issues that possibly would not have been available in the literature. These factors gave a direction in which areas the research should especially focus on when addressing supplier risk and product risk as well which factors the distribution system operators should direct attention to when as complying with NIS2 supply chain requirements. Therefore, even though as the aim of phase two

and phase three was to find out the gap that distribution system operators have when complying with NIS2 requirements, it was seen beneficial to address additional factors beyond the directives direct requirements since these were often discussed during the interviews. These factors were

1. cooperating with stakeholders
2. focusing on component level security in supply chain risk management
3. considering legacy technology contracts, especially related to strategic items that in this case are operational technology

There was also an open-ended question regarding both the mandated scope and non-mandated scope, that allowed survey recipients to add if they saw something else should be considered too.

Phase two had respondents working for the same companies that were interviewed for phase one. Phase three respondents were experts working in the same value chain with the DSOs but not directly in electricity distribution sector. As such, it was considered that they are key stakeholders of the DSOs. Phase three used the same set of questions as phase two. The goal was to broaden the perspective when conducting the gap analysis for the distribution system operators challenges with NIS2 compliance. It was estimated that the experts of phase three might have knowledge about the operational environment or supply chain that distribution system operators would not come to think about. Secondly, because phase two respondent size remained so low, phase three goal was to increase the number of respondents. A general note of the percentage variation of phase three compared to phase two is that phase three had more respondents. Thus, it is natural that the variation is higher in phase three.

5.4.1 Gap analysis according to phase two and phase three responses

As stated before, the survey questions were identical during both phases. The first question was about which measure the respondents consider the easiest in order to comply

with NIS2 requirements of supply chain and supplier management formed with the recommendations given by Traficom (2024) and FISC (2024) whereas the second asked the most challenging measure.

“Listing all suppliers and subcontractors that have an effect on the cybersecurity” during phase two was seen easy by half of the recipients whereas challenging by the other half (50/50). Since the perceptions on the ease of this measure are contrasted, it could indicate that this is a potential gap of the understanding of NIS2 requirements amongst distribution system operators. In phase three, 50% of respondents agreed that this was easy, while 13% thought it was difficult. As some of the respondents of phase three surveys worked in the IT sector in the supplier role for DSO’s, some as lawyers and some as academic researchers, this result might indicate that there is a need for unifying this measure.

“Making a risk management model according to the list with an all-hazard approach and assessing suppliers through the model” was perceived challenging by all recipients (100%) in phase two. This indicates that there is a clear gap in the ability to make comprehensive risk management strategies in the distribution system operators’ organizations. However, as it is a new requirement by NIS2, it might be perceived challenging due to that reason as well. In a similar fashion, 38% of respondents in phase three perceived it was easy to comply with while 50% thought it was difficult. This percentage suggests that the risk assessment frameworks might need to be further improved, although the respondents are more likely to be assessed than work as the buyer alias assessing party

“Assessing and considering the suppliers service providers cybersecurity practices” was also considered easy by 50% of the recipients during phase two. None had chosen it as a challenging measure to comply with. The reason why this measure was assessed as easy by the DSO’s could be that the cybersecurity practice assessments can be done mirroring cybersecurity standard such as ISO27001 as it was discussed in the interviews during phase one. During phase three this was a measure that 75% of respondents found

challenging, while 13% found it to be easy. This can be seen to be indicating a significant gap in the cybersecurity assessment tools. Although the recipients who chose this measure as challenging are not working for the electricity distribution operators, the general expertise that they have especially in the IT sector indicates that there might be a need for enhanced frameworks for assessments.

Both phase two and phase three identified “setting and documenting requirements for cybersecurity contracts” as the easiest method to comply with. 100% of the respondents in phase two and 63% in phase three evaluated this as an easy measure. The reason why this was seen especially easy in phase two could be for instance that it is a straightforward action, done by experts specialized in forming contracts, such as lawyers. Additionally, as the respondent population in phase three was higher, it allowed more variation in the answers. Although this measure was seen generally easy to comply with, it might be beneficial to set even clearer guidelines for this measure as 13% of phase three respondents evaluated this as a challenging measure.

“Considering cybersecurity risks of complete supply chain” was not chosen at all during phase two or phase three neither as an easy measure or a challenging measure. However, in the open-ended question part, where respondents were asked whether they would consider another mandated measure, one recipient of phase two wanted to stress that taking the entire supply chain into account will be the hardest measure. Although this factor was aimed to be addressed in the option “considering cybersecurity risks of complete supply chain” the fact that it was emphasized also in the open section indicates that is gap that the distribution system operators should consider when complying with NIS2.

Question 3 and 4 were asking which of the other recommended measures outside the mandated compliance would the respondents consider the easiest and most challenging to execute. During phase two the easy methods of compliance were considered to be “cooperating with the stakeholders” (50%) and “focusing on component level security in

supply chain risk management” (50%). Despite the fact that these non-mandated measures were considered easy it can be stated that they are essential in managing supply chain cybersecurity. During the interviews, transparency emerged up as a supply chain threat factor. Thus, one way to improve supply chain transparency may be through encouraging cooperation in the supply chain. 75% of phase three respondents agreed that "cooperating with stakeholders" was easy. As the recipients of phase three work as distribution system operators’ stakeholders, it can be seen generally positive that this measure is perceived easy. However, also, "focusing on component-level security in supply chain risk management," was a measure that 38% found easy even though more of the respondents (50%) found the component-related measure challenging. Therefore, it could be argued that there should be a clearer support with this area.

5.5 Recommendations

The recommendations combine perspectives from the literature, the interviews executed during phase one as well as the gap analysis from phase two and three. A condensed list of recommendations is provided in the table below.

Table 8. List of recommendations.

1. Assess the risks of managing the cybersecurity at the group company level.
2. Ensure a unified agreement of how the supplier and service provider list is done. Standards e.g. ISO27001 may serve as a framework this aim.
3. Enhance the cybersecurity practices integrated to risk assessment frameworks. Tailor the framework as suitable for assessing each supplier. The framework does not need to be as extensive regarding every supplier.
4. Enhance the frameworks of assessing and considering the cybersecurity practices utilized by the existing and future suppliers or service providers.
5. Unify the process for setting and documenting the requirements for cybersecurity in contracts. Focus especially on contracts regarding legacy technology.

6. Consider the risks of complete supply chain by at least monitoring the certifications. A good indicator may be if the first vendor requires a cybersecurity certification (e.g. ISO27001) from its subcontractors.
7. Improve the communication and collaboration with supply chain stakeholders. Share up-to-date information and industry best practices.
8. Focus especially on component level cyber security. Requiring a software bill of material may serve as a tool for this aim.

As stated in the table, it might be beneficial for the DSO's to assess the risks of managing the cybersecurity at the group company level, as it has been argued by academics that outsourcing IT and cybersecurity services can create risks for both parties, the buyer and the service provider. Regarding the recital (85) and article 21 part d and e as well as and Traficom (2024) and FISC (2024) recommendations, the electricity distribution system operators might benefit from unifying the processes, enhancing cybersecurity practices, focusing on strategically important suppliers and improving cooperation in the supply chain. The distribution system operators might benefit from having a unified agreement when creating a list of the suppliers and service providers as well as their subcontractors. Indicated by the gap analysis of phase two and three, there might be a need to enhance the DSO's understanding in how this should be done. For example, following international cybersecurity standards, such as ISO27001 might help on consolidating this process.

The distribution system operators would possibly benefit from enhancing their cybersecurity practices by paying special attention to the risk assessment frameworks that are utilized when complying with the NIS2. The gap analysis indicates that this is a factor that need a special focus on. When making a risk management model according to the list, for instance continuously and iteratively improving it can be beneficial for the organization, as the suppliers are assessed individually in the end. As it has been stated both in the literature and during the interviews, standards such as ISO27001, might be useful to use at least as a basis for creating a risk management model. Additionally, It can be useful

to tailor the risk assessment according to the business criticality of the supplier. Thus, especially suppliers of strategic and bottleneck items such as OT products and smart meters, might need to be carefully assessed.

Enhancing the frameworks of assessing and considering the cybersecurity practices utilized by the existing and future suppliers or service providers might prove to be useful in complying with NIS2. While conducting this the DSO's might benefit from consultancy from other sectors. While this measure was perceived easy by the DSO representatives, it was found challenging by other experts. As the other experts work also in the IT sector, this contrast might indicate that there might be a need for enhanced frameworks for assessments. Requiring a certification of a well-known cybersecurity standards might help in increasing trust and transparency in the supply chain. The cybersecurity practices that individual suppliers have can vary, and therefore the assessment should maybe not focus only on mirroring these to existing standards such as ISO27001, because these standards can be obtained in different levels.

Unifying the expectations and with for instance lawyers and cybersecurity experts when setting and documenting the requirements for cybersecurity in contracts might clarify the procedure. The contracts should not directly state that the supplier needs to adhere to NIS2 requirements but rather define the needed cybersecurity requirements. Although this measure was generally perceived easy in the surveys, it can be beneficial for the DSO's to set even clearer guidelines. As contracts are seen as having a major role in supply chain cybersecurity risk management the clarity of them might be crucial for both parties, buyer and supplier, to be on the same page. It might be beneficial to assess in the contracts whether the partner is a branch of a company that operates or has ownership in other countries. The DSO's could additionally benefit from focusing especially on legacy technology contracts, especially related to strategic items such as operational technology. Additionally, it might be useful to also pay special attention to the equipment that is being "left in the field" after the contracts end. A unified solution together with the equipment suppliers may be beneficial for this matter.

Additionally, highlighting the need of considering the risks of complete supply chain in the organization level as well as in the whole supply chain. This factor is related to risks stemming from going beyond the first vendor in the supply chain, and thus, it possibly not as easy to monitor. Although if the distribution system operator knows that their first vendor requires the subcontractors to be certified, it can be seen beneficial to enhance communication generally as well. Therefore, improving transparency by enhancing the cooperation and increasing the focus on the component level security in supply chain risk management can serve as useful measures in addressing the cybersecurity risks of the whole supply chain. Cooperating with the stakeholders and sharing information has been recognized beneficial in the academic literature as methods of increasing supply chain transparency. The suppliers might benefit from requiring also a software bill of material of them to be able to monitor the component security of the IT, OT and IoT products and systems they procure.

6 Conclusion

The energy sector is one of the most crucial elements of the critical infrastructure. Therefore, the cybersecurity of this sector needs to be safeguarded to avoid consequences of cyber-attacks that could lead to cascading effects. Due to the importance of the energy sector it however targeted by cyber-attacks. Therefore, the European Union has decided to update its cybersecurity policies, NIS2 being one of them. NIS2 considers the supply chain cyber risk management. As especially smaller electricity distribution system operators are considered to need help with complying with the upcoming legislation, there was a need for a guideline targeting especially the supply chain factor of cyber risk management. To that aim, this thesis was written to create a guideline for electricity distribution system operators (DSO) for the revised network and information security directive (NIS2) compliance highlighting the special cybersecurity features in their supply chains. The research method for this thesis was design science research. The content itself is a case study, focusing on two separate electricity distribution system operators. Data is gathered with interviews and online surveys from both case companies as well as external experts. The research was conducted in three phases, using both interviews and surveys as data gathering methods.

DSO's might benefit from having a unified agreement when creating a list of the suppliers and service providers as well as their subcontractors. Moreover, the operators would possibly benefit from enhancing their cybersecurity practices by paying special attention to the risk assessment frameworks that are utilized when complying with NIS2. Enhancing the frameworks of assessing and considering the cybersecurity practices utilized by the existing and future suppliers or service providers might prove to be useful in complying with NIS2. Additionally, highlighting the need of considering the risks of complete supply chain in the organization level as well as in the whole supply chain. Improving the transparency by enhancing the cooperation and increasing the focus on the component level security in supply chain risk management can serve as useful measures in addressing the cybersecurity risks of the whole supply chain.

Lack of transparency in the supply chain turned out to be a major issue in the supply chain. The methods that DSOs have to manage the risks at the supply chain level are risk assessments through frameworks by for instance utilizing international cybersecurity standards such as ISO27001, setting cybersecurity requirements in contracts and enhancing cooperation in the supply chain. The gap analysis of distribution system operators' supply chain cybersecurity management showed that both to collaborating with the stakeholders in the supply chain and forming the contracts with cybersecurity requirements were seen to be easy, whilst legacy technology contracts especially related to strategic items such as operational technology (OT) was seen difficult when complying with NIS2 requirements. When assessing different products with Kraljic matrix, OT products and systems were indeed categorized as having the most strategic importance for the distribution system operators, overruling the information technology (IT) products and systems. Additionally, Internet of Things (IoT) related products, such as smart meters, were seen to be strategically important to the distribution system operators. Therefore, the OT products and smart meters are also the riskiest when procuring them, since they are harder to replace than other products. Regarding OT products the reason is because there are fewer suppliers and the product lifecycle is long. Smart meters are also prone to become bottlenecks and acquiring them can become difficult.

The study begun before the recommendations were published. Thus, the interviews in phase one took place before that. This is considered to have a possible effect on the study quality. The low participation number of research phase two is considered as a limitation in this study. Also, the fact that this study is conducted only in Finland might affect the generalizability of the research results. One recognized limitation in this thesis is that when addressing cybersecurity standards, it focuses primarily in ISO27001, although there are other cybersecurity standards available. Therefore, when conducting further research this limitation could be acknowledged and the topic could be researched while considering other standards too. Furthermore, as the directive is transposed to national legislation, a follow up research after the national law has been set could prove to be beneficial.

References

Alhelou, H. H., Hamedani-Golshan, M. E., Njenda, T. C., & Siano, P. (2019). A survey on power system blackout and cascading Events: Research Motivations and challenges. Energies, 12(4), 682. https://doi.org/10.3390/en12040682

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219–238. https://doi.org/10.3390/jcp1020012

Balbi, S. B. V. G. N. (2019). The new frontiers of procurement in the digital age. Results of an empirical survey on procurement 4.0 in Italy1.

Benaroch, M. (2020). Cybersecurity Risk in IT Outsourcing—Challenges and Emerging Realities. In: Hirschheim, R., Heinzl, A., Dibbern, J. (eds) Information Systems Outsourcing. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-030-45819-5_13

Borenius, S., Gopalakrishnan, P., Bertling Tjernberg, L., & Kantola, R. (2022). Expert-guided security risk assessment of evolving power grids. Energies, 15(9), 3237.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, *34*(7), 342-353.

Braun, V., & Clarke, V. (2021). Thematic Analysis. SAGE Publications, Ltd. (UK).

Britannica. (2024). Retrieved 03-09-204 from https://www.britannica.com/money/business-organization

Calder, A. (2008). IT governance: A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Publishers.

Caniëls, M. C., & Gelderman, C. J. (2005). Purchasing strategies in the Kraljic matrix—A power and dependence perspective. Journal of Purchasing and Supply Management, 11(2–3), 141–155. https://doi.org/10.1016/j.pursup.2005.10.004

Cornell Law School. (2022a). Retrieved 03-09-2024 from https://www.law.cornell.edu/wex/entity

Cornell Law School. (2022b). Retrieved 03-09-2024 from https://www.law.cornell.edu/definitions/us-code.php?width=840&height=800&iframe=true&def_id=16-USC-500553564-818788136&term_occur=999&term_src=title:16:chapter:16C:section:973

Dresch, A., Lacerda, D. P., & Antunes, J. A. V. (2015). *Design science research* (pp. 67-102). Springer International Publishing.

Durst, S., & Henschel, T. (2024). Small and Medium-Sized Enterprise (SME) Resilience. Springer.

ECOFYS. (2017). Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector final report.

European Commission. (2003/361/EY). Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

European Commission. (2023). https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

European Commission. (2024a). Retrieved 15-02-2024 from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commission. (2024b). Retrieved 15-02-2024 from https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

European Commission. (2024c Retrieved 15-02-2024 from https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992;

European Union Agency for Cybersecurity (ENISA). (2021). Threat Landscape for Supply Chain Attacks. Retrieved 01-02-2024 from https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Ferguson, D.D.S. The outcome efficacy of the entity risk management requirements of the NIS 2 Directive. Int. Cybersecur. Law Rev. 4, 371–386 (2023). https://doi.org/10.1365/s43439-023-00097-8

Finnish Energy. (2024a). Retrieved 05-02-2024 from https://energia.fi/en/energy-sector-in-finland/energy-networks/electricity-networks/

Finnish Energy. (2024b). Retrieved 05-02-2024 from https://energia.fi/energiatietoa/energiamarkkinat/

Finnish Government. (2024). Retrieved 05-05-2024 from https://valtioneuvosto.fi/hanke?tunnus=LVM027:00/2023

Finnish Information Security Cluster. (2024). Retrieved 20-05-2024 from https://www.fisc.fi/sites/fisc/files/inline-files/KYBER-ALA_NIS2_OPAS_0.9_BETA.pdf

Finnish National Emergency Supply Agency. (2022). Huoltovarmuuskeskus. Toimialojen kyberkypsyyden selvitys 2022. Retrieved 03-04-2024 from https://www.digipooli.fi/sites/digipooli/files/inline-files/HVK_Toimialojen%20kyberkypsyyden%20selvitys%202022.pdf

Finnish Standards Association. (2024). Retrieved 02-02-2024 from https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

Finnish Transport and Communications Agency. (Traficom). (2024) Retrieved 20-05-2024 from https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mita-nis2-direktiivissa-esitetyt-kyberhygieniakaytannot-ovat

Fransila. (2024). Implementing NIS2 EU Directive to a Large International Company in Finland. https://urn.fi/URN:NBN:fi:amk-202404055821

Goudarzi, F. S., Bergey, P., & Olaru, D. (2023). Behavioral operations management and supply chain coordination mechanisms: A systematic review and classification of the literature. *Supply chain management, 28*(1), 140-161. https://doi.org/10.1108/SCM-03-2021-0111

Hajmohammad, S., & Vachon, S. (2016). Mitigation, avoidance, or acceptance? Managing supplier sustainability risk. *Journal of Supply Chain Management*, *52*(2), 48-65.

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., ... & Khan, A. W. (2021). Cybersecurity standards in the context of operating system: practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR)*, *54*(3), 1-36.

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., ... & Khan, A. W. (2021). Cybersecurity standards in the context of operating system:

practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR)*, *54*(3), 1-36.

Hirsjärvi, S., Remes, P., Sajavaara, P., & Sinivuori, E. (2009). Tutki ja kirjoita (15., uudistettu painos.). Kustannusosakeyhtiö Tammi.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010

IEA (2023) Unlocking Smart Grid Opportunities in Emerging Markets and Developing Economies.

International Society of Automation ISA. (2017). https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack

Johannesson, P., & Perjons, E. (2014). *An introduction to design science* (Vol. 10, pp. 978-3). Cham: Springer.

Kanstrén, T., Savolainen, P., Heino, P., & Kanstrén, K. (2017). *A study on cybersecurity industrial end-user perspectives in Finland*. https://doi.org/10.1145/3129790.3129800

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, *15*(7), 5828. https://doi.org/10.3390/su15075828

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and opportunities. *Sensors*, *21*(18), 6225. https://doi.org/10.3390/s21186225

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. Production and operations management, 31(12), 4488-4500. https://doi.org/10.1111/poms.13859

Linderoth. (2024). The impact of NIS 2 on the Swedish energy sector: A qualitative interview study about the greatest changes and challenges faced when implementing NIS 2. URN: urn:nbn:se:his:diva-23964

Maleh, Y. (2021). IT/OT convergence and cyber security. *Computer fraud & security, 2021*(12), 13-16. https://doi.org/10.1016/S1361-3723(21)00129-9

McKinsey. (2024). Retrieved 04-04-2024 from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-supply-chain

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., & Zacharia, Z. G. (2001). Defining supply chain management. *Journal of Business logistics*, *22*(2), 1-25.

Michalec, O., Shreeve, B., & Rashid, A. (2023). Who will keep the lights on? Expertise and inclusion in cyber security visions of future energy systems. Energy Research & Social Science, 106, 103327. https://doi.org/10.1016/j.erss.2023.103327

Moeller, S., Fassnacht, M., & Klose, S. (2006). A Framework for Supplier Relationship Management (SRM). Journal of Business-to-Business Marketing, 13(4), 69–94. https://doi.org/10.1300/J033v13n04_03

Monaco, R., Bergaentzlé, C., Vilaplana, J. A. L., Ackom, E., & Nielsen, P. S. (2024). Digitalization of power distribution grids: Barrier analysis, ranking and policy recommendations. Energy Policy, 188, 114083.

Monaco, R., Bergaentzlé, C., Vilaplana, J. a. L., Ackom, E., & Nielsen, P. S. (2024). Digitalization of power distribution grids: Barrier analysis, ranking and policy recommendations. *Energy Policy*, *188*, 114083. https://doi.org/10.1016/j.enpol.2024.114083

Montgomery, R. T., Ogden, J. A., & Boehmke, B. C. (2018). A quantified Kraljic Portfolio Ma-trix: Using decision analysis for strategic purchasing. Journal of purchasing and supply management, 24(3), 192-203. https://doi.org/10.1016/j.pursup.2017.10.002

National Audit Office of Finland. (2023). Retrieved 05-03-2024 from https://www.vtv.fi/blogit/tietojarjestelmien-toimittajariippuvuutta-voi-valttaa-monin-tavoin/.

Nowak, G. J. (2015). Information Security Management with accordance to ISO27000 Standards: Characteristics, implementations, benefits in global Supply Chains. *Logistyka*, *2*, 639-654.

Palo Alto Networks. (2024). Retrieved 23-03-2024 from https://www.paloaltonetworks.com/cyberpedia/what-is-it-ot-convergence

Pereira, G.I., Silva, P.P., 2017. The smart grid and distributed generation nexus. In: Castro, N., De, Dantas, G. (Eds.), Distributed Generation: International Experiences and Comparative Analyses. PUBLIT, Rio de Janeiro.

Plėta, T., Tvaronavičienė, M., Della Casa, S., Agafonov, K. 2020. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. Insights into Regional Development, 2(3), 703-715. https://doi.org/10.9770/IRD.2020.2.3(7)

Privacyengine. (2024). Retrieved 03-09-2024 from https://www.privacyengine.io/blog/iso-27001-nis2-differences/

Purser, S. Standards for Cyber Security. In Best Practices in Computer Network Defense: Incident Detection and Response; Hathaway, M.E., Ed.; IOS Press: Washington, DC, USA, 2014; pp. 97–106.

Pursiainen, C., & Kytömaa, E. (2022). From European critical infrastructure protection to the resilience of European critical entities: what does it mean? Sustainable and Resilient Infrastructure, 8(sup1), 85–101. https://doi.org/10.1080/23789689.2022.2128562

Saberi, S., Kochuzadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, Vol. 57, No. 7, pp. 2117-2135.

SANS. (2024). Retrieved 07-02-2024 from https://www.sans.org/mlp/nis2/

Sievers, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *Int. Cybersecur. Law Rev.* **2**, 223–231 (2021). https://doi.org/10.1365/s43439-021-00033-8

Smith, K., & Wilson, I. D. (2023). Critical infrastructures: a comparison of definitions. *International Journal of Critical Infrastructures*, *19*(4), 323–339. https://doi.org/10.1504/ijcis.2023.132213

Song, J. M., Wang, T., Yen, J. C., & Chen, Y. H. (2024). Does cybersecurity maturity level assurance improve cybersecurity risk management in supply chains?. International Journal of Accounting Information Systems, 54, 100695.

Syafrizal, M.; Selamat, S.R.; Zakaria, N.A. Analysis of cybersecurity standard and framework components. Int. J. Commun. Netw. Inf. Secur. 2020, 12, 417–432.

Taherdoost, Hamed. "Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview." *Electronics* 11.14 (2022): 2181.

Taylor, T. (2013). IT-OT Convergence. Public Utilities Fortnightly, 151(2), 46.

Teece, D.J. (2016). Outsourcing. In: Augier, M., Teece, D. (eds) The Palgrave Encyclopedia of Strategic Management. Palgrave Macmillan, London. https://doi.org/10.1057/978-1-349-94848-2_730-1

Teperi, A., Gotcheva, N., & Aaltonen, K. (2021). Design thinking perspective for developing safety management practices in nuclear industry. In *Elsevier eBooks* (pp. 309–326). https://doi.org/10.1016/b978-0-08-102845-2.00016-8

Termly. (2024). Retrieved 07-04-2024 from https://termly.io/legal-dictionary/recital/

Tessari, P., & Muti, K. (2021). Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations. *European Parliament, INGE Committee*, 29-30.

U.S. National Institute of Standards and Technology. (2024). Retrieved 11-01-2024 from https://www.nist.gov/cybersecurity

Upadhyay, D., & Sampalli, S. (2019). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 101666. https://doi.org/10.1016/j.cose.2019.101666

Van ’t Schip, M. (2024). The regulation of supply chain cybersecurity in the NIS2 Directive in the context of the Internet of Things. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4848048

Venable, J., Baskerville, R., 2012. Eating our own cooking: toward a design science of research methods. In: Proceedings of the 11th European Conference on Research Methods (ECRM). Academic Publishing Limited, pp. 399407

Ye, Y. (2021). Empirical investigation of kraljic portfolio matrix. *Journal of Supply Chain and Operations Management*, *19*(2), 153-177.

Zhou, C., Hu, B., Shi, Y., Tian, Y., Li, X., & Zhao, Y. (2021). A unified architectural approach for Cyberattack-Resilient industrial control systems. *Proceedings of the IEEE*, *109*(4), 517–541. https://doi.org/10.1109/jproc.2020.3034595

Zsidisin, G. A. (2003). A grounded definition of supply risk. *Journal of purchasing and supply management*, *9*(5-6), 217-224.