

Mapping Several NIS2 Directive Articles to Technical Specifica- tions for the Healthcare Sector in Sweden

Master Degree Project in Informatics

Second Cycle 30 credits

Spring term 2023

Student: Iyad Al Khatib

Supervisor: Prof. Stewart J. Kowalski

Examiner: Prof. Rose-Mharie Åhlfeldt

I dedicate this thesis

to my father, the great painter, poet, playwright, and director,
who left this world during the work on my thesis on the Sixth of May 2023,
but left a grand legacy that teaches heaps of knowledge, wisdom, and love.

To my father, whom without, none of my achievements would have been
accomplished.

Every word in this thesis is a flower, whose scent carries a lot of love dedi-
cated to you...

ACKNOWLEDGEMENTS

To all who helped me complete this

Master's degree project (120 ECTS) in Informatics
with a specialization in Data Science/Privacy, Information and Cyber
Security (PICS)- 30 ECTS

I would like to thank my thesis supervisor Professor Stewart J. Kowalski for his commitment, endless support, valuable advice, and input. His methods in mentoring, explanation, guidance, and information delivery were a major reason for completing this thesis work. He helped in giving me the required enthusiasm and positive energy at times when I was down, especially after the death of my father during the thesis work in May 2023, and after my mother had to go through an Open-Heart Surgery in June 2023. Prof. Kowalski's support, understanding, and advice were crucial to keep the work going.

I also extend my thanks to the thesis examiner, Professor Rose-Mharie Åhlfeldt, whose continuous support and wise management gave me the strength and logic to think and work. Moreover, her wisdom, compassion, and professional guidance were critical to help me pass the devastation of the death of my father during the thesis work.

I add many thanks to Prof. Ali Padyab, the master's degree project course coordinator, whose understanding, support, and advice were extremely valuable. He was of great help at all events through the thesis work, administratively and with valuable advice on content. I thank you Ali for all the support especially during the critical time after the death of my father.

I also thank my manager at RISE, Dr. Shahid Raza, whose advice and knowledge were so valuable to this work. His ability to connect the theoretical work to real-life problems added a large value to the research work in this thesis. Dr. Raza directed me to the right connection at RISE and elsewhere. My discussions with Dr. Raza were pivotal and very important for this research work. I also thank Dr. Raza for his great compassion and help during the time after the sudden and unexpected death of my father.

Finally, I would also like to thank my mother, sister, wife, son, and my brothers and friends, Nicolas Baron, Carlo Spellucci, Giuseppe Russo, Fabio Curti, Zaidoon Jabbar, Khaled Khalil, Chadi Khalil, Rony Ferzli, Talal Allam, Hassan Khalifeh, who were extremely supportive during my down time. Special thanks are to my brother and friend Bassam Kayal and all the Kayal Family, and Mahmoud Nouredine and all his family whose support was beyond description and who helped even when I did not ask for help! I also would not have made it without the love, support, and caring of my family in the USA, Dave, and Sue. They always did the best they could to lift me up to continue working and go on with life.

List of Abbreviations

ACM	Association for Computing Machinery
AI	Artificial Intelligence
bet	Utskottsbetänkande (Committee report)
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, and Availability
CIs	Critical Infrastructures
CS	Cybersecurity
CSV	Comma-Separated Values
CVEs	Common Vulnerabilities and Exposures
Dir	Directive
DNS	Domain Name System
Ds	Departementsserien (Department series)
DSP	Digital Service Providers
EC	European Commission
ECA	European Court of Auditors
ENISA	European Network and Information Security Agency
EU	European Union
EUIBAs	EU Institutions, Bodies, and Agencies
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
HD	Hard Disk
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IG	Institutional Grammar
InfoSec	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
MDR	Medical Device Regulation
MS	Member State
MSB	Myndigheten för samhällsskydd och beredskap (Swedish Civil Contingencies Agency)
NIS	Network and Information Security
NIS2	Network and Information Security 2
OES	Operators of Essential Services
para	Paragraph
Prop	Proposition
RQ	Research Question

rskr	Riksdagsskrivelse (Parliament letter)
SCB	Statistiska centralbyrå- Statistikmyndigheten (Statistics Sweden)
SFS	Svensk författningssamling (Swedish legislation assembly)
SLR	Structured Literature Review
SME	Small and Medium Enterprises
SOU	Statens Offentliga Utredning (Official investigations)
Specs	Specifications
SW	Software
TLD	Top-level-domain
TS	Technical Security
VSF	Vital societal functions

ABSTRACT

Compliance with legal instruments is vital for the survival of any organization or company in the public and private sectors. Non-compliance may result in criminal and financial penalties that can have grave effects on the indicted institution. In the field of Information Security (InfoSec), legal compliance cannot be achieved without relating the legal text of the relevant legislations to the technical realm. Therefore, it is pivotal to construe the relevant legal instruments in the correctly intended way and in good faith. The correct interpretation of InfoSec legal text plays a crucial role in finding the technical requirements for InfoSec compliance. However, interpreting legal texts can be very tedious and sometimes challenging due to several possibilities of interpretations, several non-universal definitions, amendments, and jurisprudence that make the job of security engineers and compliance auditors harder when trying to extract technical requirements for compliance. Furthermore, it is crucial to understand the hierarchy of laws especially when international laws are effective like EU regulations and directives. This thesis focuses on the NIS2 EU Directive and studies a few selected articles to find a method to transform the legal text to technical InfoSec specifications (specs) for compliance with focus on its application in healthcare critical infrastructures in Sweden. Accordingly, the thesis tries to answer the question on how to be compliant with selected Articles of NIS2 via setting technical specs for the healthcare sector in Sweden without violating legal obligations.

Because of the multidisciplinary nature of this research within the legal and InfoSec fields, the thesis adopts two research methods with the triangulation approach (blending of two methods). The first one is the qualitative research method. The data collection in this method follows the 'Document Studies' scheme since all sources for the research are documents, a few of which are legal instruments like NIS2, the Medical Device Record (MDR) and other Swedish laws. Hence, data was gathered from both public documents and other publications. After data collection, qualitative content analysis is performed. A total of 410 main documents are analyzed, where 36 were mostly considered, after adding 3 legal instruments as focal laws, including EU directives, regulations, and local Swedish laws. Each data source is analyzed and processed accordingly to serve the aims and research questions of the thesis. The second research method is the dogmatic method, and it is only referred to for the legal parts of the study since it supports law hierarchy and allows for legal interpretation techniques that are essential to analyze legal texts e.g., NIS2 articles.

The results show that there is a need to adopt the InfoSec definition by the specific standard of the International Organization for Standardization (ISO) and the International Electrotechnical Commission ISO/IEC 27000:2018. A second result is that the thesis work and focal points relate to socio-technical schemes and can benefit from their research results. A third result is that Institutional Grammar (IG) 2.0 as a framework to explain institutional text is only suitable for specific parts of the legal texts and is applied to Article 21(2)(e) NIS2. I.G. 2.0 is shown to be applicable when used with other interpretation techniques. A third result is that when looking for the transformation of the legal provisions to InfoSec technical specs, it is pivotal to be specific for the field of application (like healthcare CIs in this thesis) since laws from the application field may overlap with NIS2. In health related issues, NIS2 and the MDR are found to overlap, and this intersection is analyzed in the thesis. A consequent result is a set of technical specs on a timing scheme for reporting InfoSec vulnerabilities and incidents. The last result is a computer program tool written in Python that supports the research via aiding SMEs and other organizations to search for vulnerabilities related to their assets. This tool supports the reliability and validity of the results.

Table of Contents

ACKNOWLEDGEMENTS

List of Abbreviations

1. Introduction	1
1.1 Problem definition.....	4
1.2 Research aims and research questions (RQs)	8
1.3 Delimitations	9
1.4 Limitations and ethical considerations	10
1.5 Thesis structure.....	10
2. Background	11
2.1. Preliminaries.....	11
2.1.1. Legislation, law, directive, regulation, and rule.....	11
2.1.2. Critical infrastructure (CI)	12
2.1.3. Healthcare entity as a CI in the NIS2-Swedish context.....	13
2.1.4. InfoSec in the context of the research scope.....	13
2.1.5. Law hierarchy in Sweden	15
2.1.6. From EU directive to Swedish law	15
2.1.7. Case law	18
2.1.8. Swedish legal instruments for InfoSec	19
2.2. Research background.....	20
2.2.1. Rules and regulations vs IT	20
2.2.2. Institutional grammar (IG).....	20
2.2.3. Qualitative inquiry.....	22
2.2.4. Institutional design of cyber incidents in an EU context	22
2.2.5. Information security via several approaches: socio-technical	22
2.2.6. Legal automation.....	23
2.2.7. Legal requirements in informatics	24
3. Method	25
3.1 Approach.....	27
3.2 Sample selection: documents.....	32
3.3 Data collection.....	33
3.3.1 Systematic literature review (SLR)	34
3.3.2 Data collection for multidisciplinary work.....	38

3.3.3	Collecting documents	39
3.4	Data analysis.....	39
3.5	Reliability and validity	44
3.6	Ethical considerations.....	45
3.7	The dogmatic method for legal sources	45
4.	Results	48
4.1	Information security definition.....	48
4.2	Socio-technical aspects.....	49
4.3	IG for selected NIS2 provisions	52
4.4	Tool for vulnerability discovery and disclosure: NIS2 compliance.....	55
4.5	Legal interface.....	57
4.6	Mapping to technical specifications: tables and algorithms	58
5.	Discussion	62
5.1	Previous research.....	62
5.2	Methods and results.....	63
5.3	Ethical and societal aspects	64
6.	Conclusion.....	66
6.1	Open issues.....	67
6.2	Future work	67
	References	70
	Appendices.....	79
	Appendix 1	79
	Vulnerability Detection and Reporting Tool: Sample Primary Output.....	79
	Appendix 2.....	81
	Output of Python Tool for Compliance with Article 21 NIS2.....	81
	Appendix 3.....	83
	Legal Interpretation methods and techniques	83
	Appendix 4.....	84
	Article 21 NIS2	84

1. Introduction

There appears to be a systemic gap between security legislation and the methods used in many organizations to achieve digital transformation and their ability to interpret them to specify technical requirements for compliance with legal requirements. Digital information is a basic block for many vital fields including inter alia banking, traffic control (air, land, and sea), critical infrastructures (e.g., healthcare, energy resources, power-grids, water supplies), and life-critical response systems (e.g., natural disaster response). Such information is very valuable for individuals and organizations. This gold-like value and the growing levels of network connectivity/speeds leverage information-management to require protecting information, which is commonly noticeable in e-commerce (Susanto et al., 2011). This protection cannot be achieved without research and development in Information Security (InfoSec) that is based on relevant laws. These laws govern the legal, ethical, behavioral, and standardization aspects of security. Without law and law-enforcement, it would be impossible to achieve security in any realm within a territory, and it would be too hard to enjoy civilization (McClintock, 2020).

In the realm of EU security legislations, a very relevant and significant recent EU Directive known as the ‘Network and Information Security 2 (NIS2)’ was proposed in 2020 (NIS2, 2020) and published in December 2022 in the Official Journal of the EU as Directive (EU) 2022/2555 (NIS2, 2022) to replace Directive (EU) 2016/1148 that was known as NIS (ENISA, 2023).

The NIS2 Directive sets common security requirements to assure network and information security in the EU region and introduces significant changes to the previous NIS Directive (Biasin and Kamenjašević, 2022). It touches upon several vital aspects of the society and technology within the EU including the providers of vital/essential services, which the thesis focuses on since they can be construed to include critical infrastructures (CI) as explained further below. Hence, this work focuses on the relevant interpretation and implementation of NIS2 for CI in Sweden. All EU Member States (including Sweden) must transform NIS2 into national laws by October 2024 (NIS2, 2022). NIS2 Article 41(1) sets the dates to be 17 October 2024 for Member states to adopt and publish their relative laws that comply with NIS2, and 18 October 2024 as the date to start applying those laws. The processes to render such an implementation in Sweden is detailed in Section 2 of this thesis (Background). NIS2 decreases the risk of applying different methodologies in the EU when identifying essential/vital services (Biasin and Kamenjašević, 2022) since, unlike the NIS Directive, NIS2 does not require EU Member States to identify Operators of Essential Services (OES) and Digital Service Providers (DSP) within their jurisdictions. Therefore, NIS2 relieves EU nations from this burden when transforming it into national laws. In fact, the NIS2 proposal replaces OES and DSP with the categories entitled ‘essential’ and ‘important entities’ in its Annexes I and II (2018).

To render the analysis for all types of CI requires large volumes of work. Hence, the thesis again finds the need to limit the research to one type of CI in Sweden, which is healthcare. This limitation is motivated by the following four factors. Firstly, the Swedish public expenditure on the healthcare sector is 11% of the

gross domestic product (GDP)¹ according to SI (2021), and it is the fourth highest (102,537 million SEK in 2021) after expenditures on social protection, public administration, and enterprise and economic development (Statista, 2022). Secondly, there has been an increase in the number of cyberattacks on healthcare systems and cyber-connected medical devices during the COVID-19 pandemic reaffirming the urgency of leveraging security in healthcare (Cerulus, 2020; Schwartz, 2020). Thirdly, as healthcare gets more digitalized, cybersecurity risks increase (Lekshmi, 2022). Fourthly, Sweden ranks seventh in healthcare expenditure in the world and sixth in the EU (Macrotrends, 2023), and such ranks aid in leveraging Sweden as one of the top 10 countries to invest in, in the field of healthcare. Therefore, it would be important to keep up with that ranking of Sweden via being compliant with the new security directive to attract more investment in healthcare. In other words, a successful security attack may have huge life-critical, material, and economic consequences as well as indirect consequences including, inter alia, lowering the trust level of patients and investors in the security of the healthcare system and certain medical devices (Biasin and Kamenjašević, 2022).

At this stage, it is pivotal that the reader has basic knowledge with the differences between legislation, law, directive, regulation, and rule. If the reader is not familiar with these terms, Subsection 2.1.1 briefly introduces these terms and their related concepts.

It is important to comply with InfoSec legislation (e.g., regulations and EU Directives). This is partly because non-compliance may result in penalties. Legal compliance cannot be achieved without relating the legal text of the relevant legislations to the technical realm. Therefore, it is critical to construe the relevant legal instruments in the correctly intended way and in good faith. Such legal texts are garnering an increasing weight in requirements engineering and system development (Otto and Antón, 2007). However, interpreting legal texts can be very tedious and sometimes challenging due to the possible ambiguities, cross-referencing, domain-specific definitions, and amendments that make the job of security engineers and compliance auditors harder when trying to extract technical requirements and monitor compliance (Otto and Antón, 2007).

Furthermore, it is crucial to consider the hierarchy of laws in the process of compliance to security laws. For instance, international agreements (e.g., treaties and conventions) are ranked highest within the hierarchy of laws in most countries especially in the European and American continents i.e., international treaties are superior to domestic legal instruments including the constitutions (Gözler, 2016). The prioritization of such agreements is implemented via their transformation into national laws (Gözler, 2016). However, there are differences in such implementations depending on the region and country. In the EU region, all

¹ GDP is the total monetary value of all finished goods and services that are yielded in a country during a specified period i.e., a measure of overall domestic production (Fernandi, 2023). GDP is usually calculated annually, but some states calculate it on a quarterly or monthly bases. The Swedish Central Bureau of Statistics (Statistiska centralbyrån- SCB) also known as Statistics Sweden (“Statistikmyndigheten”) defines GDP as “the value of all goods and services produced in the country” to aid in measuring economic growth, and it publishes GDP information on quarterly basis (SCB, 2023).

Member States must abide by the EU law as a supranatural law i.e., having superiority over all other laws (Hildebrandt, 2020), because EU actions are founded on EU treaties approved voluntarily and democratically by Member States (EU, 2023). Since every EU Member State may implement EU legislation differently based on its national legal system, it is beneficial to limit the research to one EU Member state, where the expected results of this thesis are anticipated to have impact i.e., Sweden.

Regarding the consideration of healthcare as one of the CI according to NIS2, it is important to make sure that such a consideration does not contradict with local Swedish legal instruments since there could be some overlap in definitions when several legislations are considered. According to para 1 of the Swedish Act (2018:1174) on information security for socially important and digital services (Riksdagen, 2022a), vital societal functions (VSF) are in the sectors of energy, transport, banking, financial market infrastructure, healthcare (“hälso- och sjukvård”), supply and distribution of drinking water, and digital infrastructure. To decide if healthcare as a VSF (with assets and systems in Sweden) can be considered as a CI in Sweden, a further investigation on VSF shows that CI is clearly articulated by the Swedish Civil Contingencies Agency (MSB) as the “assets, systems or parts thereof located in the EU Member States which are essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions” MSB (2014:12). Hence, healthcare functionality is clearly included as part of the VSF in Sweden, and its infrastructure is essential for the maintenance of such VSF. This makes the intersection between the NIS2 Directive and the relevant Swedish legal instruments in agreement on considering healthcare as one of the CI.

Having set the major focus of the thesis on the interpretation of the NIS2 Directive Articles in relation to the healthcare sector (as a CI) in Sweden, a further degree of clarity in the thesis direction is needed to further focus the work on mapping several of the NIS2 Articles to technical specifications in the realm of security of healthcare systems in Sweden. Since more than one discipline is relevant to this work (computer science, law, and healthcare), it is crucial to investigate the interface between several legal norms that may affect the applicability and implementation of NIS2 (as explained above when investigating the overlap between NIS2 and Swedish legislations). Such a multidisciplinary work calls for looking at the intersection of the relevant legal instruments that may be complementary or conflicting when addressing compliance with the NIS2 Directive.

This aids in getting a useful interpretation of the NIS2 that would not contradict other applicable legislations. For instance, some systems/devices in healthcare use Artificial Intelligence (AI), and their security considerations must be addressed. This issue calls for looking at the interface/overlap between NIS2 and the legislations that relate to AI security in the EU and Sweden e.g., the AI Act (2021) and the Medical Device Regulation (MDR, 2017). This issue is further discussed in Section 1.2. According to Kowalski (1994), multidisciplinary work related to information security needs to be examined via several approaches including inter alia, sociology, criminology, general system theory, information system theory, and computer science. Following several of these approaches helps the investigation in getting the right interpretation of the NIS2 Articles since some of them may relate to several of these approaches. Moreover, Kowalski (1994) articulates the link between Information Technology (IT) security

multidisciplinary inquiry and culture, different methods, structure, and relevant machines. Considering these links is pivotal for the multidisciplinary work in this thesis. This is discussed more in Section 2 (Background).

In brief, the NIS2 Directive causes some disruptions in several organizations and EU Member States to implement it in a compliant way that does not conflict with other local or EU legislations. This multidisciplinary work involves keeping track of several fields in a focused manner to ensure that legal, technical (CS), healthcare, and management perspectives are considered throughout the process of investigation. This would leverage the sought results on NIS2 technical specifications to be legally compliant and operationally effective. Thus, the thesis shall investigate the interpretation and mapping of several NIS2 Articles to technical specifications from the angle of the healthcare sector (as one of the CI) in Sweden, while considering the interface/overlap with other legal instruments to articulate to the reader when such legislations would be complimentary or contradictory with the NIS2 implementations. Then, the thesis will propound several recommendations for possible solutions in the case(s) of contradictions/collisions of legislations.

The rest of this section discusses the problem related to liaising between the NIS2 Directive and technical specifications (Section 1.1), and it articulates the research aims and propounds the research questions (Section 1.2).

1.1 Problem definition

As mentioned in the introduction, there is a gap between security legislation and the methods used in many organizations to interpret them to specify technical requirements for compliance with legal requirements. The growing demand for securing digital information leverages the need for compliance with security legislations and requires that they are updated based on the growing needs and threats. One of the provided solutions is to follow security standards like inter alia ISO/IEC 27701:2019 (ISO, 2019), ISO/IEC 27032 (ISO, 2012), ISO/IEC 27002 (ISO, 2022a), ISO/IEC 27001 (ISO, 2022b), and ISO/IEC 27000 (ISO, 2018). It is worth mentioning that there are many standards for security, which can depend on the country, region, or union. Moreover, relevant challenges may arise from standard implementations. One good example to relate to (regarding the links between security standards and law) is the General Data Protection Regulation (GDPR).² Compliance with the GDPR is a challenging task for organizations due to several reasons like: (i) the complexity of organizational activities and data duplication, (ii) the lack of guidelines that could help organizations comply with the legal requirements, and (iii) the inability of the existent technical solutions that facilitate legal compliance to “identify the gaps, assess the criticality of the processing activities and the personal data they use, provide concrete solutions tailored to each organization to finally fortify its processes, and

² The General Data Protection Regulation (GDPR, 2018) is described by the GDPR.EU project as a privacy and security law drafted and put into effect on 25 May 2018 by the EU (Wolford, 2023). The GDPR imposes privacy obligations onto any organization so long as it targets or collects data related to people in the EU, and it imposes hard fines and penalties against whoever violates those privacy and security standards (Wolford, 2023).

guarantee the protection of individuals' personal data" (Diamantopoulou et al., 2019).

Diamantopoulou et al. (2019) argue that the ISO 27K standard series constitutes a utilizable cornerstone for organizations to build a compliance strategy via considering risk definition, risk assessment, ongoing evaluation, and relevant documentation. Furthermore, the GDPR and ISO/IEC 27001:2013 (ISO, 2013) both aim at strengthening data security, mitigating security risks of data breaches, and requiring organizations to ensure the CIA-triad (Diamantopoulou et al., 2019). On the other hand, Diamantopoulou et al. (2019) conclude that being ISO 27001 certified does not satisfy full compliance with GDPR but is a starting point. This is because ISO standards are global i.e., they are not solely made for the EU. In addition, GDPR compliance is mandatory in the EU, while standard certifications are not (Diamantopoulou et al. 2019). At the same time, Vidich (2023) articulates that the ISO/IEC 27701:2019 (ISO, 2019) extends ISO/IEC 27001 to aid organizations comply with evolving regulatory requirements since it includes an annex that comprises operational controls mapped against corresponding GDPR requirements. This mapping provides a good example of how to implement privacy regulations relative to ISO/IEC 27K standards.

It is important to note that although the ISO/IEC 27701:2019 standard helps organizations towards GDPR compliance, it still does not comprise all GDPR requirements since establishing official GDPR compliance requires EU regulators' approval (Vidich, 2023). Diamantopoulou et al., (2019) adds that not all technical security requirements to achieve privacy as articulated in the GDPR are included in the ISO/IEC 27K family. Choucri (2023) discusses the challenges of relating the text of the GDPR to applications and to generating the connections among several of its articles.

Consequently, while policy and law makers put effort on creating the required legislation to provide order and protection, the technical implementation that must comply with such legal instruments may still lack behind, especially in the first period after issuing a legislation. This can be due to several reasons like, among others: (i) timing issues, (ii) lack of clear understanding of the meaning of the legal codes, (iii) unclear relations between the articles of the same legislation (Choucri, 2023), (iv) overlap of several legislations, (v) lack of knowledge on reading legal instruments by technicians and some managers, and (vi) sometimes the absence of laws that should control some technical aspects e.g., lack of privacy protection fines based on codes like the unavailability of the GDPR in the EU before 2018 (Tessian, 2021).

In this respect, several original works have been conducted to aid organizations to implement institutional rules via the specification for encoding and analyzing institutional design e.g., Institutional Grammar (IG) 2.0 (IG, 2022) as discussed by Frantz and Siddiki (2021). IG 2.0 is an already established approach, and it can aid in encoding policy information in institutional statements via a predefined set of syntactic components (Frantz and Siddiki, 2022). Further explanations on IG 2.0 are articulated in Section 2 (Background) if the reader was not familiar with this approach. Even though approaches like IG 2.0 are available, there is still some confusion in construing legal codes to map to low-level technical specifications (e.g., computer-based specs). This confusion does not exclude legal codes in security regulations and directives like NIS (2018) and NIS2 (2020). For instance, para 15 in NIS2 (2020:16) reads the following as a legally binding requirement for organizations in EU Member States:

“Upholding and preserving a reliable, resilient and secure domain name system (DNS) is a key factor in maintaining the integrity of the Internet and is essential for its continuous and stable operation, on which the digital economy and society depend. Therefore, this Directive should apply to all providers of DNS services along the DNS resolution chain, including operators of root name servers, top-level-domain (TLD) name servers, authoritative name servers for domain names and recursive resolvers” (NIS2, 2020:16).

One research problem arises when interpreting the NIS2 text (like the above one) to follow up to several levels of analysis of language to map to technical computer science terms that would fit in compliance with relevant legislations in the Swedish Code of Statutes (Svensk författningssamling- SFS) e.g., SFS (2022:508) and other legal instruments in the EU e.g., the AI Act and MDR. Textual deconstruction of language can be considered in the linguistic philosophical meaning as described by Jean-Francois Lyotard (Lyotard et al., 2020: 327-355), where it uses fragmentation then defragmentation to the technical terms and via going through every word of the meaning while having in context all the previous works and related works to this article. For instance, what would “upholding and preserving a reliable, resilient and secure” (NIS2, 2020:16) DNS (Domain Name System) mean in technical terms when a manager needs to communicate this legal ‘wish’ to a system administrator, who is not experienced in reading legal text? How to relate it to the context of healthcare CI? Would it relate to encryption specs for network packets and Hard Disk (HD) drives in cases of adversarial intrusions? If so, would a full HD encryption be needed or is file encryption enough, and which encryption algorithm is good/best to utilize based on the size of data and time of day (traffic load) knowing that it contains healthcare records, let alone the discussion on processor power, and power consumption (also related to cooling when such issues relate to Medical Data Centers). When such questions are answered, other legal instruments need to be considered.

It is essential to remind the reader, at this stage, that the NIS2 Directive is relevant to the healthcare sector (as discussed earlier). Hence, its healthcare security requirements need to be specifically interpreted in the right way in the context of this work. Moreover, the NIS 2 Directive mandates every EU Member State to establish security measures for relevant entities. Hence, Sweden must establish security measures for healthcare CI under a Swedish scope. To do so, NIS2 Chapter IV contains the legal obligations on security, risk management, and reporting. NIS2 Article 18 states that essential and important entities (i.e., CI) “shall take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk presented” (NIS2, 2020:45).

Measures include inter alia risk analysis, incident handling (e.g., prevention, detection, and response), business continuity and disclosure. These issues require thorough interpretation within the Swedish legal system to see how their time limits, budgets and application can be implemented in a compliant manner to local laws and other EU legislations like the MDR. For instance, the MDR and NIS2 include obligations on incident notification. Article 87 MDR requires medical device manufacturers to report serious incidents to the relevant competent

authorities, while Article 20(1) NIS2 requires EU Member States to oblige essential/important entities (e.g., healthcare CI) to send the notifications of significant security incidents without undue delay. Despite the different definitions in both legislations, applying both can lead to overlapping work for medical device manufacturers. In fact, the problem is in the interpretation of both obligations in the case of overlap. One aiding factor is Article 2(6) NIS2 that articulates the case when incident notification overlaps with another specific law (legislation specific to the application e.g., MDR), and it explains that the specific-sector legal-codes should prevail if “those requirements are at least equivalent in effect to the obligations laid down in this Directive” (NIS2, 2022:31). The problem in the interpretation here lies in the vague phrase “at least equivalent,” which requires extra work to correctly identify and relate specifications to, especially that NIS2 does not explain what the word ‘equivalent’ refers to in this context, and it does not give examples of such handling.

Another type of problem that relates to the divergence between the MDR and NIS2 when mapping the legal code to technical specs is when the issue of time is to be interpreted. For instance, Article 20(4)(a) NIS2 mandates notification “*without undue delay and in any event within 24 hours after having become aware of the incident*” (NIS2, 2020:47). On the other hand, Article 87(3) MDR mandates the notification “*not later than 15 days after they become aware of the incident*” (MDR, 2017:73), Article 87(4) MDR mandates that if the event is serious then the reporting should be “*not later than 2 days after the manufacturer becomes aware of that threat*” (MDR, 2017:73), and Article 87(5) MDR mandates that in the cases of death or serious deterioration of a person’s health the “*the report shall be provided immediately after the manufacturer has established or as soon as it suspects a causal relationship between the device and the serious incident but not later than 10 days after the date on which the manufacturer becomes aware of the serious incident*” (MDR, 2017:73). In studying the above few examples, it is clear that the MDR and NIS2 are not compatible nor are they equivalent. One problem in such a situation, when transforming NIS2 to a national law in Sweden and looking at the healthcare sector as a CI, is to use interpretation approaches to come up with a legal obligation that can be put in practice without leading the organization to violations of any of the legislations.

In the last example on the time of notification, the problem of mapping of NIS2 to a specification would be to find the right number of days/hours as a maximum period before reporting to the relevant authorities without violating any other relevant legislation. Several similar conflicts of obligations are problems that this thesis will tackle. To achieve the sought results, this work divides the problem into several subproblems and tries to tackle each problem at a time to converge to the final solution and propound recommendations. The division of subproblems include, but is not limited to: (i) reviewing the NIS2 Directive and identifying the specific Articles that are relevant to the healthcare security in Sweden, (ii) breaking down every selected Article into individual objectives and obligations, (iii) investigating whether IG 2.0 and other approaches could be utilized in such a work, (iv) translating/mapping such obligations/objectives into technical controls or specs that are practically deployable in healthcare organization computer and IT systems in Sweden, (v) validating the resulting technical specs/controls to ensure legal compliance with the NIS2 Directive and other relevant Swedish and EU legislations (e.g., SFS 2022:508, MDR), (vi) communicating the resulting mapping to managers and technical personnel in a clear and

concise manner, and (vii) investigating the monitoring/auditing of the implementation of the resulting table of technical controls/specs via investigating several monitoring models or tools to ensure the ongoing compliance of the healthcare organizations in Sweden that use such controls/specs with the NIS2 Directive.

One more problem relates to whether the available NIS2 Articles are good enough to follow up with the current and near future security requirements, which can also be policy requirements. Therefore, there is a need to design a method to aid healthcare organizations in Sweden in understanding the relevant NIS2 Articles, the consequent obligations they impose, and the related standards for corporate compliance with local and EU legislations.

Furthermore, multidisciplinary work is needed to tackle the abovementioned subproblems since they belong to several fields (computer science, management, security, healthcare, and law). This issue of multidisciplinary work shall be controlled via focusing on the needed issues in every field (e.g., in the healthcare sector, the focus is on healthcare legislations in the EU and Sweden) as well as the overlap between different legal instruments as discussed above. The work in Kowalski (1994) aids in making the multidisciplinary approach beneficial, focused, and more effective.

The contribution of this thesis is in mapping few selected NIS2 Directive Articles, (that can be construed to relate to healthcare Critical Infrastructures) to specifications in the healthcare sector in Sweden. This finding provides a guiding method to healthcare providers to understand and interpret those NIS2 selected articles. Accordingly, the Articles can be mapped to practical and applicable controls that would not contradict with other legislations. Therefore, organizational compliance with the NIS2 Directive can be achieved. One major motivation behind tackling this problem is the limited period to implement the NIS2 Directive as a national law in Sweden and other EU Member States (NIS2, 2022). Hence, this is a timely issue to investigate.

1.2 Research aims and research questions (RQs)

This research aims at finding a systematic way to map selected articles of NIS2 to InfoSec technical controls and specifications for the healthcare sector in Sweden. One subgoal is to assess the use of IG 2.0 and other encoding techniques to realize a method to construe the NIS2 legal codes and relate them to technical specs. According to Smedinghoff (2008), there is a need to consider a high-level view of the multitude of security laws and regulations and summarize the global legal framework for InfoSec that relates to them, because companies struggle to comply with several InfoSec laws in many jurisdictions. Hence, another subgoal for this research is to consider both the high-level NIS2 articles within their legal/policy frameworks and the low-level technical controls/specs formulation for the specific field of healthcare in Sweden. A third subgoal is to translate legal obligations into technical obligations under the Directive (NIS2) while not allowing the overlap with other EU legislations to diverge to conflicts in implementing technical controls. This shall be done with a projection to a set of near-future legal instruments e.g., the implementation of NIS2 Directive as a Swedish law that does not conflict with other Swedish or EU legislations. A fourth subgoal is to find an approach that companies/organizations can utilize to communicate NIS2 Articles to managers and technical developers in a manner that helps understanding what they need and be legally compliant.

This poses the following research questions (RQs):

RQ1. *How to map selected articles of the NIS2 EU Directive to technical specifications for the healthcare sector in Sweden?*

- This question comprises mapping NIS2 articles to specifications that can be comprehended by managers and technical personnel without missing legal requirements that may lead organizations to violate NIS2 obligations.

RQ2. *What interpretation methods are required to encompass the new information security realities?*

- This question comprises investigating available methods (e.g., IG 2.0) that aid in deconstructing and interpreting selected legal statements in NIS2 and other relevant legal instruments (e.g., MDR) to avoid conflicts of laws in a way that is viable enough in the foreseeable future.

1.3 Delimitations

NIS2 includes one hundred and forty-four (144) preamble paragraphs, forty-six Articles, and three (3) Annexes. While the Articles are mainly regulative, the preamble paragraphs are comprised of constitutive statements describing preliminary issues that are needed before reading the articles. Annexes I and II are also either constitutive statements or definitions, while Annex III is a correlation table showing the links between the previous and current NIS directives. Hence, the thesis excludes the preamble paragraphs and Annexes from the study and focuses only on several selected Articles. The choice of the Articles is based on their relevance to:

- (i) security vulnerabilities, which are one of the major topics of concern in NIS2.

In this regard, the NIS2 Articles that this thesis focuses on are Articles 7(2)(c) which refers to Article 12(1), Articles 11(3)(a), 11(3)(b) & 11(3)(e), Articles 12(1)(c), 12(2), 12(2)(c), and 21.

- (ii) timing issues in relation to incident reporting since it is crucial for not violating time limits after security incidents occur.

Mainly, Article 20(4)(a) is investigated.

The motivation behind these choices is twofold. Firstly, they are pivotal in helping organizations become compliant with NIS2. Secondly, they relate to the aim of reducing (and possibly eliminating) the risks of conflicts of laws, which was discussed above especially in the overlap with the MDR. It is worth mentioning that excluding the preamble articles and the Annexes has no negative effect on the quality of this work.

The thesis uses the term Information Security (InfoSec) and does not use the term Cybersecurity since InfoSec is more fitting to this work. InfoSec is used in the thesis with its wide meaning to include the assets, networks, time limits, and all what relates to securing information. A delimitation in this regard is that the

thesis studies InfoSec for healthcare as one type of the critical infrastructures that are defined by the Swedish law as discussed above.

1.4 Limitations and ethical considerations

The first limitation relates to the short time provided to conduct multidisciplinary research that inquires an EU directive like NIS2. It requires more than the given time to fully consider all NIS2 articles and their intricate relations. This is why several articles are selected to tackle the research questions and show that the transformation of provisions to technical InfoSec specifications for healthcare CIs is possible and can be reliable.

The research method type adopted is qualitative ‘Content Analysis’ (Section 3.1). It is used for a topic directed at legal issues. Then it is vital to keep the standard of considering only the relevant laws, looking for related ones, and conducting interpretation in good faith.

In addition, when the research is directed to the healthcare sector, ethical considerations are important especially in keeping thorough checks on the technical specifications required by the legal instruments.

1.5 Thesis structure

The rest of this thesis is organized as follows. Chapter 2 presents the background needed for the research work. Chapter 3 describes the research method. Chapter 4 deliberates the results. Chapter 5 provides an overall discussion in relation to previous sections (previous research, methods, implementation, results, and relevant ethical/societal aspects). Chapter 6 concludes the thesis.

Appendix 1 shows a sample output of a Python tool developed during this thesis work. The sample shows how vulnerabilities are detected so that they can be reported with a sample program output. In the sample in Appendix 1, the thesis attempts to show that a computer programmable tool can be developed to support the compliance to the selected NIS2 articles (i.e., implementation of the legislation).

Appendix 2 presents and discusses the output of another module of the Python tool for compliance with Article 12 NIS2. This output sample shows correlations of healthcare vulnerabilities with other IT specifications.

Appendix 3 lists the legal interpretation methods and techniques, of which a few were selected for the interpretation phase in the thesis work.

Appendix 4 shows Article 21 NIS2, which is the one selected as a sample of interpretation in Chapter 4 on results.

2. Background

This thesis work is multidisciplinary and relates to the fields of Informatics and law while focusing the application in the healthcare sector. Hence, this section includes reviewed literature that relates to these disciplines. Moreover, some reviewed sources will be explained in more detail than others since they relate to the background needed for the reader to easily understand relevant materials for different sections of the thesis.

The rest of this chapter is organized as follows. Section 2.1 presents the preliminaries that are needed for the reader to grasp the remaining of the thesis, and Section 2.2 discusses the research background that was conducted earlier within the relevant fields.

2.1. Preliminaries

This section presents the main concepts that the reader needs to apprehend for the rest of the work. If the reader is familiar with any of the concepts that are presented in this section, she/he may want to jump to the next section.

Since the thesis deals with legal instruments, the first concept explains the differences and relations between legislations, laws, directives, regulations, and rules (Subsection 2.1.1). Moreover, the work focuses on healthcare critical infrastructures, hence, the second concept to present is that of Critical Infrastructure (Subsection 2.1.2). Afterwards, the discussion continues to the concept of considering a Healthcare entity as a CI in the EU and Swedish perspectives (Subsection 2.1.3). Then, the text elaborates on Information Security within the context of the thesis scope (Subsection 2.1.4). Furthermore, the hierarchy of laws in Sweden is explained (Subsection 2.1.5) since it is essential to understand before discussing the effect of NIS2 (as an EU directives) on the Swedish legal norms. Once the hierarchy concept is well perceived, the exposition clearly articulates the transformation of an EU Directive into a Swedish law (Subsection 2.1.6), which is a pivotal process to grasp since it is one of the motivations for doing this research work and since it locates the research focal points (see Figure 8). Case law is also briefly introduced so that the reader can grasp the concept of its relevance to this work and future works (Subsection 2.1.7). Finally, Subsection 2.1.8 presents the Swedish Legal Instruments related to InfoSec.

2.1.1. Legislation, law, directive, regulation, and rule

Legislation is the process of creating laws by some governing entity (Cornell Law School, 2022). Hence, there are several types of legislation e.g., directives, laws, regulations, and decisions. A directive is a class of legislation used in the European Union (EU) that sets binding goals for all EU Member States, but to put it in practice, it must be transformed to a national law in each Member State (EU, 2022). A law is the set of binding rules and principles that govern the behavior of individuals and organizations within a territory or country (Cambridge, 2022), and it is made by parliament bodies or similar law-making bodies e.g., congress in the USA (The White House, 2022) and “Riksdag” (parliament) in Sweden (Ministry of Justice, 2016). A regulation is a binding legislative act with specific rules created by administrative/regulatory agencies of a government to implement and enforce laws (Merriam-Webster, 2022). In this respect, an EU regulation is a type of binding EU legislative act that must be applied with direct effect

in its entirety across all EU Member States (EU, 2022). A rule is a specific regulation or guideline issued by an administrative agency (e.g., Department of Energy, schools, universities) to specify how a specific aspect of a law should be practically implemented in a place or situation (PEO, 2022). Accordingly, laws always apply to all people within a jurisdiction while regulations only affect those who deal with the agency that enforces them. Rules can lead to consequences for the group that violate the rule without any effect outside the group even if this rule was broken by someone outside the group.

In this regard, it is important to comply with InfoSec legislations (e.g., regulations and EU Directives). This is partly because non-compliance may result in penalties. Legal compliance cannot be achieved without relating the legal text of the relevant legislations to the technical realm. Therefore, it is critical to construe the relevant legal instruments in the correctly intended way and in good faith. Such legal texts are garnering an increasing weight in requirements engineering and system development (Otto and Antón, 2007). However, interpreting legal texts can be very tedious and sometimes challenging due to the possible ambiguities, cross-referencing, domain-specific definitions, and amendments that make the job of security engineers and compliance auditors harder when trying to extract technical requirements and monitor compliance (Otto and Antón, 2007).

Furthermore, it is crucial to consider the hierarchy of laws in the process of compliance to security laws. For instance, international agreements (e.g., treaties and conventions) are ranked highest within the hierarchy of laws in most countries especially in the European and American continents i.e., international treaties are superior to domestic legal instruments including the constitutions (Gözler, 2016). The prioritization of such agreements is implemented via their transformation into national laws (Gözler, 2016). However, there are differences in such implementations depending on the region and country. In the EU region, all Member States must abide by the EU law as a supranatural law i.e., having superiority over all other laws (Hildebrandt, 2020), because EU actions are founded on EU treaties approved voluntarily and democratically by Member States (EU, 2023). Since every EU Member State may implement EU legislation differently based on its national legal system, it is beneficial to limit the research to one EU Member state, where the expected results of this thesis are anticipated to have impact i.e., Sweden.

2.1.2. Critical infrastructure (CI)

It is important to note that the terms 'Critical Infrastructure' and 'Industrial Network' are often confused with each other although they are used in limited contexts (Knapp and Langill, 2015). An 'Industrial Network' relates to any network that includes an automated control system communicating in a digital fashion with other components, while a 'Critical Infrastructure' refers to the critical systems and assets included in a computer-networked infrastructure (Knapp and Langill, 2015).

Due to the overlap between the two definitions, confusion between the two terms exists. Furthermore, the overlap and confusion cause the problem of leaving many critical infrastructures at risk of security attacks nowadays (Knapp and Langill, 2015). This is because assets are not highlighted in the consideration of the 'Industrial Network' definition. For the thesis interest, only the term 'Critical Infrastructure' (CI) is used as per its above definition since it aids in relating NIS2 Articles to CI security vulnerabilities via the consideration of assets as part

of the CI definition. In other words, when systems and assets are considered in CI, the related vulnerabilities can be an immediate outcome to be aware of to protect such systems and assets from possible threats/attacks.

When dealing with the concept of CI in general, several regional and national policies as well as laws identify and prioritize CIs comprising key resources to assure a legal bases for their protection against security attacks (e.g., terrorist attacks). Such legal instruments construe CI to include any entity or service whose disruption may affect a nation's economy, security, or health. Examples include, among others, energy sources, power plants and grids, nuclear energy, chemical factories, agricultural services and plants, pharmaceutical companies, medicinal manufacturing and distribution, hospitals, and healthcare organizations (Knapp and Langill, 2015).

2.1.3. Healthcare entity as a CI in the NIS2-Swedish context

It is important to clarify that healthcare is not always defined within the legal instruments as one of the CIs. For instance, NIS left this issue for the EU Member States to define which sectors are included. However, NIS2 relieves Member States from this burden in its Annexes I and II. In fact, the overlap between NIS2 and the Swedish law consider healthcare entities as CI. This issue was discussed above in more detail (see Section 1 'Introduction'). In brief, the first paragraph (para) of the Swedish Act (2018:1174) on InfoSec for socially important and digital services considers vital societal functions (VSF) to be included in the healthcare sector ("hälso- och sjukvård"). In addition, CI is clearly articulated by the Swedish Civil Contingencies Agency (MSB) to include "health" (MSB, 2014:12). Consequently, healthcare functionality is part of the VSF in Sweden, and healthcare infrastructure is essential for VSF maintenance.

2.1.4. InfoSec in the context of the research scope

The concept of InfoSec has been used in many texts for different purposes, and it has become a trendy term so that not all its definitions are professional in the context of Informatics. To grasp the scientific concept of the term and deploy it research methods to be used in research work like this thesis, its definition needs to be articulated clearly. The thesis considers the concept of InfoSec discussed by the ISO/IEC 27000:2018 standard, which presents related terminology within which its Section 3.28 defines InfoSec as the "*preservation of confidentiality, integrity and availability*" (CIA) of information (ISO, 2018:3.28). These three aspects are known in security as the CIA triad (Death, 2017). Other properties can be related to these aspects such as authenticity, accountability, nonrepudiation, and reliability (ISO, 2018). However, these properties do not stand alone like the CIA triad.

The authors in Åhlfeldt et al. (2007:2) further simplify the gasping of these aspects by articulating their aim to deliver "the right information to the right people in the right time." In the context of this thesis, delivering secure information to the right people is interpreted to add the need to dispense it 'to the right place.' Thus, the thesis sees this definition to imply that secure-information management is needed. Then the quest to understand the concept of InfoSec forks to how CIA-triad can be protected i.e., securing CIA with the highest level possible depending on information value. Thus, it is crucial to grasp the meaning of each of the three concepts of the CIA-triad and how they relate to each other.

Confidentiality is understood as the property of information not being disclosed and not made available to unauthorized parties or processes (ISO, 2018). Integrity is defined as the “property of accuracy and completeness” (ISO, 2018). It pertains to safeguarding against undesired changes (Åhlfeldt et al., 2007). Therefore, it relates to the ability to trust saved/received information. Availability is articulated as “being accessible and usable on demand by an authorized entity” (ISO, 2018:3.7). Hence, it relates to the anticipated use of resources within a period (Åhlfeldt et al., 2007). The CIA triad concepts reveal the desired aims. A note worth mentioning is that all the CIA-triad concepts are similarly important. However, sometimes they must be balanced against each other depending on circumstances e.g., confidentiality can have a higher priority when the value of the relevant data depends on limiting access-to-data (e.g., electronic health records).

Åhlfeldt et al. (2007) present the InfoSec Model that aids in grasping the concepts of InfoSec and the CIA triad. This model shows how other security properties relate to InfoSec in a top-down approach. The scope of InfoSec ensures the CIA of information and entails applying (and managing) appropriate controls. These controls should consider many threats, and at the same time they have two aims. The first aim is achieving sustainable business success and continuity. The second aim is minimizing the effects of security incidents (ISO, 2018). Hence, to achieve InfoSec it is good to implement an applicable set of controls. These controls are selected through the chosen risk management process. Moreover, they are managed using an Information Security Management System (ISMS). This includes policies, procedures, processes, organizational structures, software (SW), and hardware to protect assets (ISO, 2018).

Security controls are divided into Administrative Security and Technical Security (TS). TS is also divided into IT Security and Physical Security (which is out of the scope of this thesis). Cybersecurity (CS), as a term, is still used in a broad manner with varying definitions that are usually written with a subjective view. Therefore, they can be somehow uninformative (Craig et al., 2014). This is a reason to slow down the desired progress in InfoSec. Nonetheless, a set of definitions is available in industrial standards like National Institute of Standards and Technology 2013 standard (NIST, 2013) and ISO/IEC 27032:2012 (ISO, 2012) that relate CS to the CIA triad. Furthermore, other definitions are provided in research works. For instance, Craig et al. (2014) define CS via focusing on organizations. On the other hand, von Solms et al. (2013) discuss other perspectives like personal, societal, and national issues.

After understanding the concepts related to InfoSec as discussed above, it is important to note that InfoSec and CS concern a whole nation since security attacks threaten Critical Infrastructures (e.g., hospitals and electric plants). CS is aligned with business purposes, monetary assets, economic information, and monetary assets that are connected to other networks. Hence, external dependencies exist and affect business goals. Accordingly, they need security. CS has a broad context. InfoSec considers all information threats. Thus, it is related to CS at the systems-management level. Moreover, a thorough investigation of entities outside the organization is needed to check the type of external requirements in relation to other factors like customers, suppliers, etc. Nonetheless, this thesis needs to deal with InfoSec, knowing that CS is closely related to InfoSec. However, the term InfoSec is the one used throughout the thesis.

2.1.5. Law hierarchy in Sweden

This subsection relates to the discussion in Section 2.1.1, which articulates the differences between legislation, law, directive, regulation, and rule. Having discussed these terms and relieved the confusion related to their use for the reader, this subsection follows up by presenting the hierarchy of laws in the Swedish legal system. This is pivotal to make it possible to grasp the concepts related to InfoSec regulations in Sweden that are presented below in Subsection 2.1.7.

Carlson (2013) clearly elaborates the hierarchy of laws in Sweden, where EU law is the supranatural law. EU laws are then followed in rank by: (1) the constitution (“grundlagar”), (2) legislation (“lagstiftning”) including “parliamentary acts (lagar), government regulations (also referred to as ordinances, *förordningar*) and agency regulations (*föreskrifter*)”, (3) legislative preparatory works (“*förarbeten*”), (4) Case law (*rättspraxis*”), (5) General principles of law (“*allmänna rättsprinciper*”), (6) “Custom and usage,” and (7) legal scholarship or doctrines (“*doktrin*”) (Carlson, 2013:42).

2.1.6. From EU directive to Swedish law

Inasmuch as the previous section is important to aid in grasping the concepts of regulating InfoSec in Sweden, this subsection is essential for subsequent sections especially in relating NIS2 to the context of the Swedish legal system.

Riksdagen (2021a), Riksdagen (2021b), Riksdagen (2022a), Riksdagen (2022b), Regeringskansliet (2021), Regeringskansliet (2022), EC (2016), EC (2022a), and EC (2022b) show how an EU legislation (e.g., EU Directive) is transformed into a Swedish law. Figure 1 presents the process of transformation with all its sub-processes, and Figure 8 shows the focal points of the thesis within these sub-processes. The sub-processes are articulated in the following text.

Being an EU Member State (MS), Sweden has transferred part of its right to make decisions on legislation to the EU (Riksdagen, 2021a). However, after an EU legislation is enforced, the Riksdag decides whether this legislation is to be implemented in Sweden and how to do so (Riksdagen, 2021b). When the Council of Ministers and European Parliament adopt an EU legislation (e.g., a Directive), it must be incorporated as a national law into every EU MS to apply (Riksdagen, 2021b).

A Directive sets out the desired objectives and lets the Member States decide on the implementation method to achieve the sought objectives. On the other hand, EU regulations apply directly in the same way in all EU Member States (Riksdagen, 2021b). Hence, the Riksdag (Swedish parliament) is responsible for implementing EU legislations in Sweden as national laws. The way that the Riksdag works in such a matter is like its procedure in adopting laws originating from Sweden.

The Swedish legislative process (*lagstiftningsprocessen*) starts with the government rendering official investigations known as SOU (*Statens Offentliga Utredningar*), after which the government sends an SOU referral (“*Remiss*”) to referral bodies e.g., authorities, organizations, municipalities, and other stakeholders (Regeringskansliet, 2022).

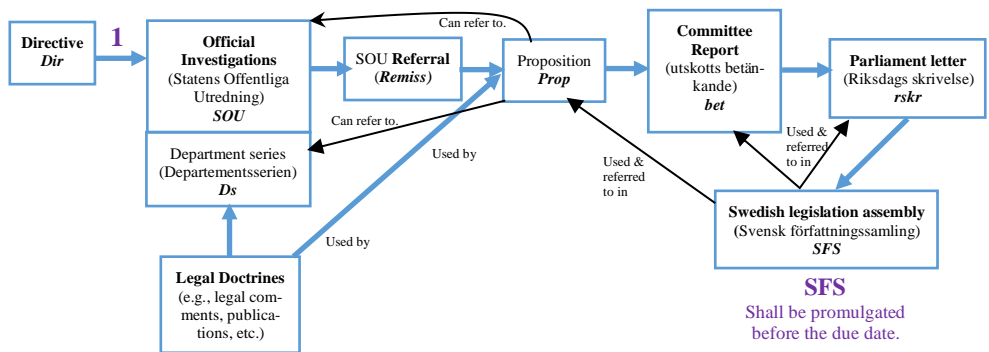


Figure 1. The legislation process from an EU Directive (point 1- when the EU Directive is published) to a Swedish Law (SFS point- when an SFS shall be promulgated before the due date).

The opinions of the referral bodies are processed by the relevant governmental offices (Regeringskansliet, 2021). Both the referral bodies, and the relevant governmental offices need relatively long periods to render this hard work (Regeringskansliet, 2021). All responses from referral bodies are published on a website and included in the basis for any following decisions on the referral (Regeringskansliet, 2022). Then, the government studies the replies from the referral bodies and writes a bill/proposal (“proposition”- referred to in legal databases as ‘prop’) to the legislative council (“Lagrådet”), which has judges from the Supreme Administrative Court and the Supreme Court of Sweden. The legislative council investigates if any legal problem exists in the proposal e.g., contradicting the constitution or other applicable laws, regulations, or rules (Riksdagen, 2022b). After receiving the replies, the government re-writes the proposal and submits it to the parliament (“Riksdagen”).

Since each parliamentary year the government sends around 200 proposals to the parliament (Riksdagen, 2022b), the deadline to produce relative national law becomes more time-pressuring. The Chamber of the Riksdag decides on a law or an amendment to the law after the proposal is processed by a committee (“utskott”) based on the committee’s responsibility. There are fifteen committees. Every committee is specialized in some areas of responsibility (Riksdagen, 2022b). The committee members are comprised of several parties in the parliament, and the committee invites experts/representatives from other organizations for their opinions. The hearings on the proposal are sometimes open to the public. The committee checks if the proposal is consistent with other legislation and complies with the committee’s previous notes given to the government on the matter. Then, the committee submits its suggested proposal (“förslagen”)—based on the views of the majority of its members— to the parliament (Riksdagen, 2022b). Committee members with dissenting opinions may submit their reservations. Then, the parliament takes the suggested proposal (“förslagen”), prepares a relevant report (“utskottsbetänkande”— referred to in legal databases as ‘bet’), and sends it to the members (“ledamöter”) to read it (Riksdagen, 2022b) so that they can decide on it either directly or after a debate. After members are done with the debate, the speaker (presiding over the chamber) asks the chamber

to vote on the proposal following a voting protocol that accepts a majority vote consisting of more than half of the votes. The parliament then sends a short message/letter (“Riksdagsskrivelse”- referred to in legal databases as rskr) to the government informing of the decision (Riksdagen, 2022b). When the vote is decided, the parliament decides on a new law.

Then the governmental duty is to ensure the publishing of the law in the Swedish legislation assembly (“Svensk författningssamling”- referred to in legal databases as SFS), where each SFS has the year of publication and the number of the decision in that year (Riksdagen, 2022b). Then, the Swedish government must implement the new law, where the ministries, state authorities, and some companies aid in the process since they are subordinates to the government. For instance, in the case of a law related to healthcare decisions, the National Board of Health and Welfare (“Socialstyrelsen”) is an example of such aiding authorities, where the government specifies the guidelines for their work. In Sweden, the ministerial rule (“ministerstyre”) is not allowed (Riksdagen, 2022b) i.e., the government cannot decide how the authorities’ ongoing work should be done.

Finally, the parliament follows up on the implementation of the law via a process starting with a report submitted by the government on a yearly basis to the parliament stating the measures it took to implement the law (i.e., the letter may include the measures on various decisions). Then the Constitution Committee processes the letter, and the Chamber debates it (Riksdagen, 2022b). If the parliament is not satisfied with the governmental processing of the new law implementation, it can call on the government to take other measures via an announcement (“tillkännagivande”). Moreover, the parliament’s committee evaluates how a new law has worked in practice via continuous following up (Riksdagen, 2022b).

At the same time, since the European Commission (EC) is referred to as the ‘guardian of the treaties,’ it is responsible for ensuring that all EU Member States properly apply EU legislation (EC, 2022a). The EC supports all the above national processes via online information, expert group meetings, implementation strategies, and guidance documents e.g., online Frequently Asked Questions (EC, 2022a). The EC guidelines aid EU Member States in the transposition for EU Directives and application of EU Regulations starting right after the adoption of the legislation (EC, 2022a). Moreover, the EC takes measures if a Member State does not fully integrate an EU Directive as a national law by the deadline or if the Member State had not applied the EU legislation correctly (EC, 2022a). The details of these measures are articulated in EC (2016). The different tools used by the EC to ensure that EU legislation is properly applied to meet its main objectives (i.e., people/businesses benefit from the commonly agreed rules in the EU, as soon as possible) are presented in EC (2022b) including prevention and sanctions. Details on monitoring the implementation of EU Directives as well as reporting on performance of EU Member states in such matters are discussed in EC (2015). In cases of infringement to an EU directive, the procedure of the EC is detailed in EC (2019).

The abovementioned references are pivotal for the investigation in this thesis. This is because there exists a fixed number of months (21 months) starting from the day the NIS2 Directive entered into force (16 January 2023) as published by the European Network and Information Security Agency (ENISA) until NIS2 must be transformed into a national law on 17 October 2024 (ENISA, 2023). This transformation to national laws is an obligation on all EU Member States (NIS2, 2022). Hence, the Swedish parliament, government, and relevant referral bodies

face time pressure and other problems that may be alleviated by the work in this thesis.

2.1.7. Case law

Case law relates to courts and court decisions. It is also one source to investigate in relation to the implementation and scope of applicability of an EU Directive. Figure 2 shows how court decisions provide the relevant case law (jurisprudence) that can be referred to by the SFS legislation, and how such case law can affect doctrines and future cases. Although case law is important in the study, the thesis scope will not focus on considering cases since the research aims at investigating provisions in the NIS2 directive in relation to specifications. However, this subsection is important so that the reader is well informed about the relationship between case law and the regulation (SFS) that would be a final national legal instrument that results from the EU Directive, NIS2. Nonetheless, the following paragraph provides brief information on which courts and organizations monitor and audit EU Directives. Figure 2 illustrates how Courts and case law relate to the process of transforming an EU Directive to a Swedish law and this serves the location of thesis focal points that are shown later in Figure 8 (in Section 3).

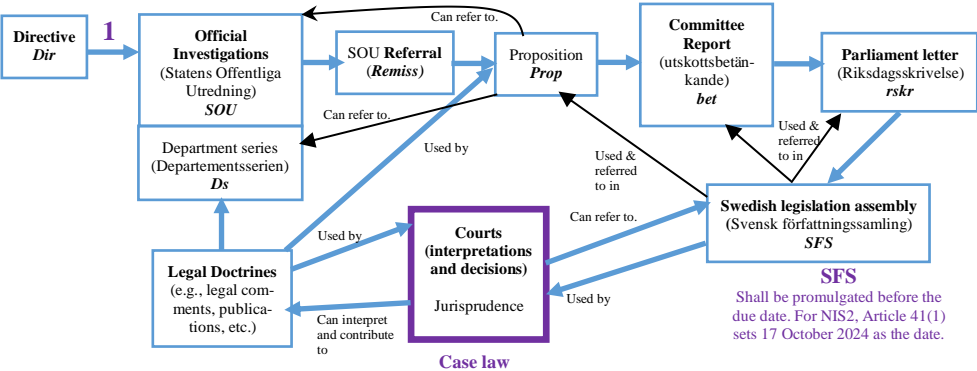


Figure 2. The legislation process from an EU Directive (point 1) to a Swedish Law (SFS point) and the relationship to Case law, which are outcomes of Court Interpretations and decisions (jurisprudence).

In this regard, the auditing of effectiveness, efficiency, legality, and regularity of EU actions including EU Directives is to a large extent provided by the European Court of Auditors (ECA), whose goal is “to improve accountability, transparency and financial management, thereby enhance citizens’ trust and respond effectively to current and future challenges facing the EU” (ECA, 2023: para 7). The ECA Review No 02/2019 entitled “Challenges to effective EU cybersecurity policy” provides an overview of the complex cybersecurity policy, lists major challenges to effective policy delivery, and covers information security as well as cyber defense and disinformation (ECA, 2019). Moreover, the ECA’s Special Report 05/2022 examines if the EU institutions, bodies, and agencies (EUIBAs) have implemented adequate arrangements to protect against cyber-attacks (ECA, 2022). The report found that the level of preparedness is not in proportion with the threat and recommended that the EC improves EUIBAs’ preparedness

via introducing binding cybersecurity rules and increasing resources for the Computer Emergency Response Team (ECA, 2022).

2.1.8. Swedish legal instruments for InfoSec

Every EU Member State has already passed through the phase of transforming the NIS Directive to a national law. The process of transforming an EU Directive into a national law is discussed in detail in Subsection 2.1.6.

Sweden, being an EU Member State, implemented the related Swedish law on information security for socially important and digital services (SFS 2018:1174), known in Swedish as “Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.” This law is the most related to NIS2, which is enforced in January 2023, thus it also needs to be transformed into a national law. Article 1 (§1) SFS 2018:1174 deliberates the aim of the law and articulates the relevant fields that are divided into two categories: (1) socially important services in the sectors of “energy, transport, banking, financial market infrastructure, healthcare, supply and distribution of drinking water, and digital infrastructure,” and (2) digital services (SFS, 2018:§1). Hence, healthcare is one of the sectors that the law aims at providing it with a “*high level of security within information systems and networks*” (SFS, 2018:§1)

There are also other legal instruments for InfoSec in Sweden such as the Protective Security Act (2018:585), which referred to in Swedish as Säkerhetsskyddslag (2018:585). This law concerns entities that conduct activities of importance to security in Sweden or activities “covered by an international commitment on security protection that is binding on Sweden” as well as entities that “intends to transfer shares or shares in security-sensitive operations and on international cooperation in the area of security protection” (SFS, 2018b:§1).

Furthermore, the Swedish legal system includes government regulations (also referred to as ordinances, *förordningar*) and agency regulations (*föreskrifter*) that describe a lower granularity of detail for compliance with the law. Some of the related regulations is ordinance (2018:1175) on information security for socially important and digital services, which supplements the law (2018:1174) related to NIS (SFS, 2018c). In the Swedish legal system, this regulation is referred to as *Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*. This regulation aids organizations via detailing the data protection and preventive measures as well as the way to deploy them. Another regulation is Security Protection Ordinance (2018:585), which is referred to in the Swedish legal system as *Säkerhetsskyddsförordning (2018:658)*. This regulation “contains supplementary provisions to the Security Protection Act (2018:585)” (SFS 2018d:§1).

When it comes to organizations and firms, internal rules also provide a lower level of detail to comply with the regulations and laws. The focus of this thesis is on Small and Medium Enterprises (SMEs) since they share the same interest as all other organizations to be compliant with the NIS2 but have fewer resources to interpret the Directive and laws to map it to technical specifications.

In this regard, a very important governmental agency that provides information, material, methods, and support to organizations and firms to be compliant with security laws in Sweden is the Swedish Civil Contingencies Agency (MSB).

2.2. Research background

This section discusses what other research has been conducted within the thesis research field. Several research efforts have gone through the muddy waters of the gap between security legislations and their practical interpretations for implementation. This review explores previous work that is useful for the work in this thesis. Some of the reviewed literature comprises existing research that studies relevant parts of the problem area. The presented previous background relates to rules and regulations in relation to information technology, Institutional grammar that is an inductive method to interpret institutional rules, institutional design of cyber incidents in an EU Context, several information security approaches, legal automation, and Legal Requirements in Informatics i.e., including InfoSec. A short summary of the reviewed literature is presented in Table 2. For further details, the reader may want to hop to the text that directly follows Table 2.

2.2.1. Rules and regulations vs IT

Zalnieriute et al. (2019) explores the tension between the rules and regulations on one side and the fast technological development to conclude that automation can have two effects on governmental decision-making. It can enhance it and detract from the rule of law values. It aids this research in building upon its observations to evaluate whether automation of legal code translations would uphold the basic ideals of the rule of law when its outcome is a list of technical specifications.

2.2.2. Institutional grammar (IG)

The work on Institutional Grammar 2.0 (Frantz and Siddiki, 2021; Frantz and Siddiki, 2022) relates to encoding and analyzing institutional design. It is very interesting to investigate for the sought work in this thesis since it relates to analyzing institutional rules/text in a formal way to eventuate in a scientific understanding of the text and a better interpretation that is coherent with what the institutional rule is intended for. In brief, IG 2.0 specifies an integrated syntax for capturing information that is articulated in statements that are regulative and/or constitutive. Such statements are used in institutions to represent rules. IG 2.0 allows for the operationalization of the syntax of the text, which is what makes it intriguing for this work. An interesting point is that it divides the text into basic units, where the unit of analysis is the instructional statement. Each statement describes expected actions. It considers the actions to be directed for actors (the intended audience of the instructional statement that is required to understand and employ the statement). Moreover, the expected actions are described in the instructional statement within contexts.

In this respect, IG 2.0 parametrizes the features of an institutional system within contexts. In other words, the context is used together with the breakdown of each institutional statement to extract features of the institutional system and map them to useful parameters. This strikes a chord with the work intended in this thesis; however, this thesis analyzes legal text and not institutional text. Therefore, some caution is needed in relating the literature review on IG 2.0 to the thesis work. Nonetheless, some analogy in the methods may prove useful during the course of the investigation. Back to the type of statements, below is a brief description of the two types: regulative and constitutive statements.

IG 2.0 Regulative Statements describe actions for an audience of specific actors within certain contextual parameters. Each regulative statement is composed of attributes (actor with relevant behavior regulated by the statement), aim (activity, goal, or outcome), context (conditions that instantiate statement or qualify action), object (entity that is targeted/affected by particular action), deontic (articulates statement action if compelled, restrained or discretionary), and an ‘or else’ part (includes consequence of violating the statement). For instance, consider the statement “Organic farmers must comply with organic farming regulations immediately following certification, or else face revocation of organic certification” (Frantz and Siddiki, 2022:12).

In decomposing the statement to its basic parts based on I.G., the statement is composed of attributes, deontic, aim, direct object, and implied context, which are organic farmers, must, commit to, organic farming standards, and under all conditions, respectively (Frantz and Siddiki, 2022). The statement does not include an ‘or else’ part or value combinations. Furthermore, the statement “Organic farmers must commit to their organic farming standards and accommodate regular reviews of their practices” (Frantz and Siddiki, 2022:12) comprises distinctive activities and associated objects. They “commit to organic farming standards” and “accommodate regular reviews of their practices.” The decomposition of the statement results in having attributes (Organic farmers), deontic (must), aim (commit to; accommodate), direct object (organic farming standards; regular reviews of their practices), and implied context (under all conditions). This fragmentation of the regulative statement is used to interpret the intended meaning and result in having correct and practical parameters that the audience (actors) need to understand and deploy. Below is a simple example to illustrate the deconstruction of a regulative institutional statement to its components (Frantz and Siddiki, 2022:16):

<u>Attributes</u>	<u>Deontic</u>	Aim	<u>Direct object</u>
<u>“Organic farmers</u>	<u>must</u>	commit to	organic farming standards.”

IG 2.0 Constitutive Statements parameterize features of a system, and they are made of constituted entity (constituted in the statement), constitutive function (expression linking the entity to institutional setting), context (clause capturing conditions expressing applicability of statement, or qualify the constitutive function), constituting properties (linked to entity as mediated by the constitutive function), modal (operator signaling necessity, possibility, or impossibility of the constitution specified in the constitutive function), and an ‘or else’ part (articulating the consequence of violating the statement) (Frantz and Siddiki, 2022). An example of a constitutive statement is “Starting January 1, the Department of Agriculture is the certifying authority, or else the organic program cannot be administered” (IG, 2022:1). The entity is the Department of Agriculture, the constituting property is being the certifying authority, and the consequence of violation (or else) is that the organic program cannot be administered. This is another example of the fragmentation of a statement, but of the constitutive type, to end up in a better interpretation for the intended audience (actors) of the statement. This approach is worth trying in the cases of legal statements in this thesis work.

2.2.3. Qualitative inquiry

In Creswell et al. (2016), the authors discuss qualitative inquiry. It articulates how characteristics of the qualitative method have several different ways to construct a mapping to technical controls/specs via capturing the meaning that the stakeholders need to follow. This work is relevant and useful to the methodology work of this thesis and can serve as a good basis for the analysis part. It can also partially aid in the way of interpreting the effect of the supranatural nature of the EU law when translating high-level Directive Articles to the technical levels.

The work in Thombre (2019) explains the Golden rule of interpretation which, in brief, can be summarized by following the text, word-by-word, and analysing it via linking to other legal texts, customs, norms, conditions, and relevant previous work of the text. The aim is to interpret the intention of the text. This is an important rule and will be useful for the investigation.

2.2.4. Institutional design of cyber incidents in an EU context

The work in Kianpour and Frantz (2021) analyzes institutional design of EU cyber incidents correctly considering the supranatural power of EU laws. This is a very interesting work for this research since it shows the variable degrees of polycentricity in EU security regulations for governance. It also points toward potential limitations of the compliance mechanisms in relation to delegations of sanction specification. It constitutes a good basis for the high-level analysis part. It can also be used to take into consideration the supranatural nature of EU law when translating such high-level rules to the technical levels. It can be useful also to add the resulting technical specifications to be useful for crises management.

2.2.5. Information security via several approaches: socio-technical

The work in Kowalski (1994) tackles the problem of securing information via using several approaches e.g., IT system theory, computer science, sociology, criminology, and General System Theory to develop a model for socio-technical security systems for protecting information handled by IT. This model helps focus the analysis into four areas: ethics, politics and law, operations and management, and technology. All these areas are relevant to this thesis work. Nonetheless, the area of politics and law is most relevant since Kowalski (1994) studies the development of national IT systems security evaluation criteria and relates the criteria to IT crime cases. This issue is relevant to this thesis investigation and will be considered. Moreover, the conceptual model created and presented in Kowalski (1994) as the Security by Consensus (SBC) model is interesting to study if it can be related to this thesis work. The IT insecurity problem is formulated in Kowalski (1994) as an emergent property of socio-technical systems that exists at all levels of socio-technical systems comprising the international, national, organizational, and group-individual level (see Figure 3).

Kowalski (1994) argues that an organization can develop administrative policies that guidelines that mitigate security risks. Then, at the national system level, new IT components can be produced, and new laws can be issued to have better control and minimize InfoSec risks. According to Kowalski (1994), these measures can be taken at different levels of a socio-technical system e.g., international, national, organizational, and group-individual level (see Figure 3). However, depending on the case studied and its circumstances, there could be a problem of identifying at which level an IT security measure should be taken.

One issue that relates to this thesis work is that at the national level (e.g., Sweden), there is governmental concern with InfoSec vulnerabilities, procedures, supplies, users, legal interpretations, requirements setting, implementation, and testing. Further discussion on these points in relation to the results of this thesis is articulated below in Section 4.2.

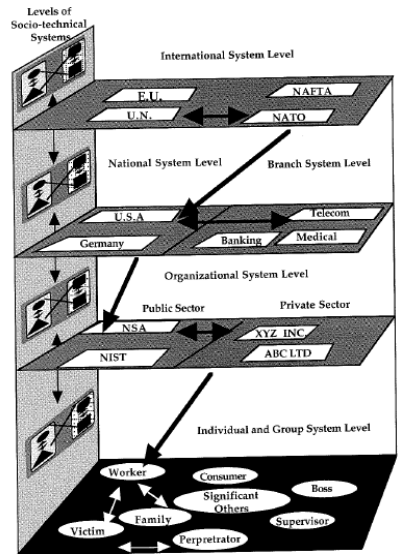


Figure 3. System of socio-technical systems (Kowalski, 1994:fig.1.8). Permission to use this figure in this thesis is granted by the author of Kowalski, (1994).

2.2.6. Legal automation

In Pasquale (2019), the author eloquently discusses the issue of legal automation, which is the field of using computer algorithms to automate the work of legal practitioners as well as trials of automating legal decisions. The author discusses the fear of eliding or excluding important human values and characteristics that are needed in legal interpretation e.g., improvisations, irreducibly deliberative governance, narratively intelligible communication (especially needed for due process). The paper discusses how such commodities are not reducible to SW and computer algorithms. Pasquale (2019) explains how language is constitutive of all aspects of law and stresses that preserving accountability and a humane legal order requires expressing law in a human language by a responsible person. This basic requirement for legitimacy besides the fact that legal automation (nowadays) is still not well developed to carry on tasks as the one to conduct in this thesis, then this proposal agrees with Pasquale on the limitations of legal automation in several contexts including inter alia contracting, property recordation, and – most importantly- corporate compliance. Since a robust, ethical, and human-based legal profession must respect the basic prerequisites for legal language, which are flexibility and subtlety, for an accountable and fair social order, this thesis sees that legal automation is not at a stage to consider in the analysis. Thus, one of the delimitations of the thesis is to not consider legal

automation. A very important reason for this is also articulated in Pasquale (2019) that the success in technologies for legal automation are still limited to aiding in some help to legal practitioners e.g., speeding up their searches, document writing, decision-making, and tax-form filling. Hence, this success only ensures the success of persons in the legal field and not machines, yet. Although legal automation is an interesting and probably promising field, the thesis work does not consider it useful for the investigation.

2.2.7. Legal requirements in informatics

In Otto and Antón (2007), the authors survey research papers (from 1957 till 2007) that address legal requirements in requirements engineering. The reviewed papers handle legal texts for developing systems that include symbolic logic, programming logic, first-order temporal logic, deontic logic, defeasible logic, goal modelling, and semi-structured representations. This survey is directed to requirements engineers and auditors. The aim is to help such audiences to have better specifications, enhance system monitoring, and test the compliance of SW systems. The difference between the aims of the surveyed papers and the aim of this thesis is that the paper targets SW systems while the thesis has a narrow scope of transforming the legal text to technical specifications. However, several surveyed papers serve to compare (by analogy) the work done in addressing legal text for technical requirements and compliance.

Moreover, it is of interest to look at the difference between legal codes (e.g., NIS2 Articles) and the issue of justice i.e., questioning if the compliance imposed on companies would be just if some Articles are too hard to deploy. This calls for looking partly into the works of Michel Foucault on law, who saw some injustice and control in some laws (Foucault, 1975) as well as irregularities in relation to laws through history (De Ville, 2010). Moreover, Lyotard's view on pluralism in writing laws is valuable to achieve justice via taking multiple views into consideration while writing or interpreting a law since he calls for the rule of divergence rather than convergence (Kebede, 2002). Such works may help the investigation in having open mindedness towards other legal instruments that may apply when interpreting the NIS2 Articles e.g., the AI Act and the MDR.

Although the focus of this research is on the NIS2 Directive Articles (NIS2, 2020), the NIS Directive (NIS, 2018) is part of the literature review that aids in comparative legal studies to better interpret NIS2 and check the lessons learned and see where enhancements are needed and included.

3. Method

Conducting research requires applying a research methodology, which is a step-wise process to make sure that the results and scientific knowledge created are up to the standard required by the scientific community. Hence, everything claimed in the end would be new and everything discovered is traceable, reliable, and valid. This section discusses the research methods adopted in the thesis and their relevant choices.

This work is multidisciplinary, where the research renders investigations within the fields of Informatics (focusing on InfoSec) and law (e.g., EU regulations and directives). Within these two disciplines, the focus is on healthcare critical infrastructures in Sweden (as an EU Member State). This calls for the implementation of two research methods. The first method is chosen to fit the Informatics discipline, and the second method relates to legal analysis. Figure 4 shows the two fields and their respective research methods.

Since the interest of this research work aims at understanding the interpretation of selected Articles of NIS2 and relating them to InfoSec technical specifications, then the most fitting method is the qualitative method, which is discussed in detail below.

The second method is the dogmatic (doctrinal) method since it is commonly used in legal analysis. It is centered around a system of recognized legal sources/documents (Hutchinson and Duncan, 2012). Its main objective is to establish a systematic exposition of the principles, rules and concepts of a particular law or legal field, interpret the law, and analyze the relationship between laws and legal principles (Smits, 2017). This approach provides a solid structure to enable a thorough explanation of legal rules (JHLL, 2019) since it comprises law hierarchy and legal interpretation methods that are useful when reading legal codes and trying to understand their purposes and meanings (Kilcommins, 2015).

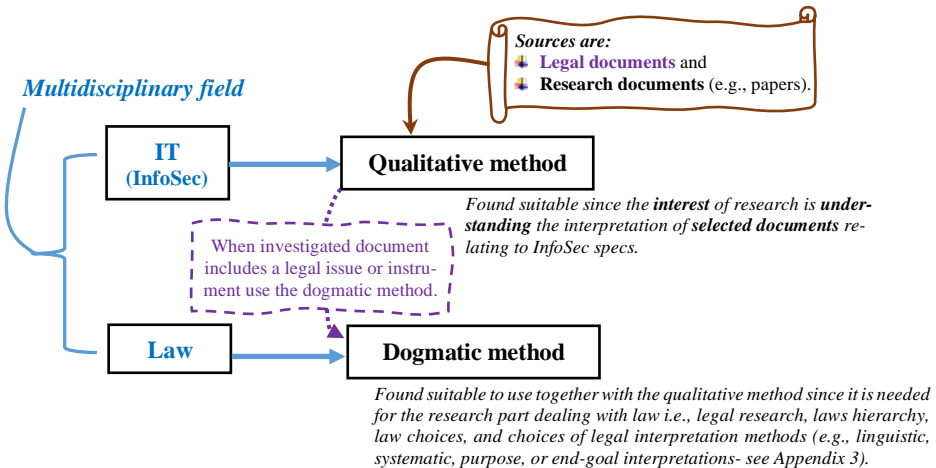


Figure 4. Research Methods used in this multidisciplinary research comprising the IT field (InfoSec) and law. The qualitative method is chosen to fit the IT discipline, & the dogmatic method relates to law. An example of a shift from the qualitative method to the dogmatic one (purple dashed-line inscribed text) is when IG 2.0 is used to deconstruct a text and part of it needs legal interpretation or analysis (see further discussion in Subsection 4.3) .

After introducing the needed methods for the multidisciplinary research, it is noteworthy to discuss why these research methods fit the thesis investigation. In this respect, the solid structure (organization of legal components) provided by the dogmatic approach aids in understanding and setting the legal hierarchy between different legal instruments before starting the investigation. This is important since the hierarchy setting (when using the dogmatic method) aims at determining the order of authority of the investigated laws before the investigation starts. For instance, NIS2 (as an EU directive) and the MDR (as an EU regulation) have a higher priority (authority) than any local law in any EU Member State. Thus, if a legal obligation is set by these EU legal instruments, it would supersede any conflicting obligation in any national law in EU Members States. However, if a conflict is shown to exist between EU laws (same hierarchy), then it cannot be neglected. It better be treated by legal analysis techniques that the dogmatic method allows and provides. Hence, the dogmatic method is used in this thesis as an aiding approach to the qualitative approach in three ways: hierarchy of laws, choices of laws, and using legal interpretation methods. Figure 4 shows how the dogmatic method aids the qualitative approach when the investigated document (source) is a legal instrument.

The dogmatic method is briefly discussed in this thesis since it relates to the legal part while the focus of the thesis is on InfoSec (even though NIS2 is a legal instrument) i.e., the focus of this discussion is on the qualitative approach.

The qualitative research method fits this work since it is suitable for the thesis aims, and choosing a research method that meets the research purpose is an important factor according to Streubert and Carpenter (1999). The qualitative approach is also appropriate when a complex problem needs recognition via garnering deep comprehension as well as pointing out the problem from different angles (Crowe et al., 2011). This method aids in understanding the high-level socio-technical aspects as well as specifications in the technical realm. Hence, the work uses this methodology to explain the gap between laws (from a social perspective) and technical requirements. It also aids in proposing socio-technical improvements for best practices. In brief, the socio-technical aspects within the qualitative methodology are very enriching for the research. This is the type of mind-set that requires investigating social sciences and available InfoSec/IT developments and tools. The qualitative methodology supports such multi-dimensional work, where not only one view is correct (due to the social aspect). In other words, there is not going to be only one objective view of reality since laws change, and they remain connected to culture, ethics, society, technology, and other human related issues. When there is a human in the blend, social issues become evident. Hence, thorough investigations in the socio-technical realm are needed. Qualitative research aids in understanding how InfoSec has been shaped by the people working in it and how it affects their methods of work i.e., interactions between different fields.

Furthermore, the qualitative methodology supports looking at the described phenomenon from different perspectives, and it aids in opening new realms to enrich the research e.g., investigating whether the use of IG 2.0 would be applicable to this work. One aspect of the qualitative research method that can relate to all the disciplines in this work is the data collection. Data can be collected from different resources like technical documents, research documents (e.g., papers), other publications, data from companies (not available in this thesis work), and legal documents/instruments (e.g., NIS2). This methodology supports changing

the way of investigation via looking at the data from different angles and by not sticking to one way of investigation. This allows for the smooth shifting between the qualitative method and other methods e.g., dogmatic method (see Figure 4 and Figure 5). For instance, if NIS (2018) was problematic within the work, some shift to NIS2 (2020) or other rules can be investigated. Inductive data analysis can be used to find patterns and categories. In addition, the qualitative method allows the researcher to understand a problem or phenomenon from the perspectives of the people it involves i.e., managers, technical personnel, and law-makers. This betters the picture of the research problem and proposed solution. The qualitative methodology also supports in-depth descriptions for interpretation by using documents, personal experiences, or observation. The characteristics of the qualitative method aid in utilizing the participants' meaning so that when people have different ways in understanding the mapping to technical controls, the focus would be on learning the meaning that the stakeholders need to understand (Creswell et al., 2016). Moreover, emergent design can be used as one characteristic since the research will follow an iterative approach so that research processes can be refined. The research may use social, cultural, political, or historical contexts.

'Interpretive inquiry' is an important characteristic of qualitative methodology that is used in this work, where, firstly, text interpretation is rendered based on the golden rule of interpretation as described in Thombre (2019). This golden rule avoids anomalous and absurd understanding of the law due to literal (word-by-word) (Thombre, 2019).

One more characteristic of this method is the 'Holistic account' to develop a fathomable picture of the problem at hand and identify the complex interactions of socio-technical factors that affect the phenomenon. This is because if the phenomenon is removed from the local settings (organization and jurisdiction), then it would not be the same phenomenon. Hence, the qualitative method aids in keeping in mind the value of the context/settings that can oftentimes be company related (e.g., when implementing standards). The qualitative methodology will also be helpful in using grounded theory i.e., inductive processes when needed. Moreover, the iterative process in the qualitative research methodology will help the work to continue until it reaches the thesis aims.

The rest of this chapter is organized as follows. Section 3.1 deliberates the research approach. Section 3.2 discusses the sample selection of documents. Section 3.3 elaborates on the data collection. Section 3.4 analyzes the data and discusses the analysis procedures. Section 3.5 investigates the reliability and validity aspects of the research. Section 3.6 articulates the research ethical considerations.

3.1 Approach

The research questions and aims (discussed above in Subsection 1.2) give a hint to the choice of research approach. The major aim of the research is to find a systematic way to map selected articles of NIS2 to InfoSec technical controls and specifications for the case of the healthcare sector in Sweden. This aim is evaluated and the relevant subgoals are inferred. In this regard, the subgoals help divide the main aim into smaller objectives that aid in reaching this very aim (Berndtsson et al., 2008). For instance, one subgoal is to obtain the right and relevant documents.

In this respect, it is important to differentiate between documents that are legal instruments and all other types of documents included in the research. As Figure 4 shows, when a legal document is to be investigated, a large part of the work may revert to the dogmatic method, which is discussed briefly in Section 3.7 (below). Hence, while locating documents, both the qualitative method and the dogmatic method are used. The qualitative method is used for all types of documents; however, when there is a need to choose a legal document, find its legal hierarchy, or choose a legal interpretation method, then the dogmatic method is used based on the steps described in Section 3.7.

Back to the subgoal of obtaining relevant documents, it is divided into several steps like locating the following types of documents, among others: (i) the enforced version of NIS2 in English and Swedish- if available- since several proposals were published earlier, (ii) relevant Swedish laws (in Swedish and- if possible- with formal translations to English like those within the “Riksdags” databases/resources), (iii) court decisions and opinions, (iv) legal doctrines like official legal comments and legal publications (see Figure 2 that shows how doctrines relate to the studied process), (v) timely technical standards, and (vi) timely and relevant research publications.

Another subgoal example is the interpretation of NIS2 with institutional and legal interpretation methods to see which of these methods best fits the main aim (discussed further in Chapter 4). This subgoal needs to use both research methods, the qualitative and the dogmatic. This is because the institutional interpretation (using IG 2.0) reverts to the qualitative approach, while the legal interpretation requires carrying the legal instrument (e.g., NIS2) and reverting to the dogmatic method and the consequent legal analysis techniques allowed by this method. Examples of such legal interpretation techniques are linguistic, systematic, and purpose based interpretations (see Appendix 3 for other methods of legal interpretation). This calls for a third subgoal since investigations need to determine whether IG 2.0 would prove satisfactory for the thesis aims.

Accordingly, the third subgoal is to assess if the use of IG 2.0 would be valid and reliable to realize an inductive method to construe the NIS2 legal codes and relate them to technical specs in InfoSec. Hence, in setting this subgoal, it becomes clearer that inductive reasoning is needed in the approach. It is noteworthy to mention that not all documents are legal and public, but only a few are. Inductive reasoning is used on all documents (sources). However, when reading the legal documents relevant to this research (e.g., NIS2 and MDR), there are two steps to accomplish the task of finding relevant IG 2.0 attributes in these documents to fit the research work. The first step to start with is the qualitative research approach with inductive reasoning; nonetheless, this calls for content analysis to understand the meaning and value of the content. After rendering the first step, the result would be several legal phrases or statements, which require legal interpretation i.e., requiring a second way/step of analysis. This second step uses legal techniques (allowed and provided by the dogmatic method), which can be inductive and reductive. Examples of such techniques are extensive interpretation, restrictive interpretation, and analogies (i.e., induction and reduction). It is worth mentioning that this thesis does not utilize the technique of opposite interpretation (*e contrario*), which is rarely used in legal interpretation (Bernitz, 2020).

After having set the subgoals, it becomes clearer to choose the ‘type’ and ‘sub-type,’ of the qualitative approach, that best suit this thesis investigations. Since

inductive reasoning is required, then this hints to look at the types of the qualitative approach that would support inductive reasoning as well as document analysis. Accordingly, it is important to check the kind of documents (sources) that are investigated. Since the work investigates primary documents (e.g., research articles, publications, and legal instruments) to converge to results (as a second phase) after analyzing these documents, then the best fitting type of the qualitative approach is the ‘secondary research’ (George, 2023). According to Bhandari (2023), this choice is fitting since it collects “existing data in the form of texts, images, audio or video recordings,” and it allows for inductive reasoning (see Figure 5). Hence, secondary research is applicable to the above-mentioned research questions, whose purpose is to induce information from previously existing (primary) documents and come up with information about links to technical specifications. These links can be categorized to explain what technical specs to link to i.e., to answer the research questions on the ‘what, why, and how’ (Crowe et al. 2011).

Utilizing the qualitative ‘secondary research’ type with inductive reasoning is needed in this thesis work when moving from the available sources (documents) in a step-by-step deconstruction to defragment the studied text and conclude some meaning. Hence, this deconstruction is needed to arrive at the required technical specifications e.g., when using IG 2.0. In such a scenario, a document would be investigated with inductive reasoning, however, if some part(s) of the text under deconstruction includes legal statements, then the analysis forks to the dogmatic method to aid in the legal reasoning and interpretation as shown in text inscribed within the purple dashed-line in Figure 4 and Figure 5.

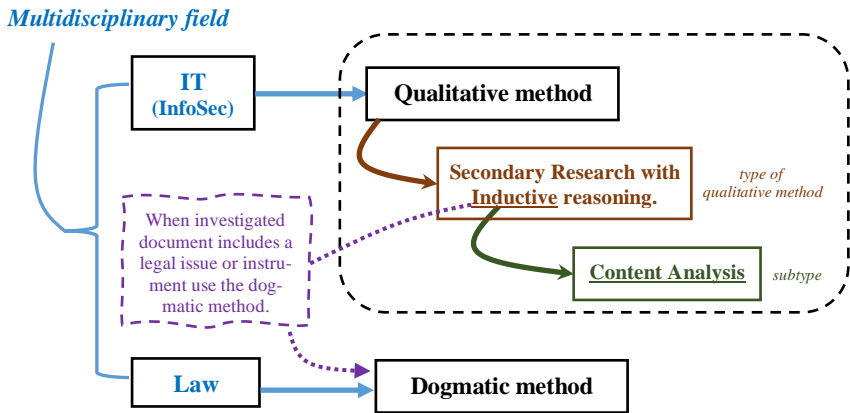


Figure 5. Research approach showing the type (brown colored text) and subtype (green colored text) of the qualitative research approach, which fit the research work. At the inductive reasoning stage, the approach may fork to either the subtype of qualitative ‘Content Analysis’ or to the dogmatic method if the document, statement, or phrase investigated at a certain stage (step) required legal analysis, hierarchy setting, or interpretation techniques.

After having chosen the suitable type of the qualitative research approach (‘secondary research’), it is also important to determine the best fitting subtype under the umbrella of ‘secondary research.’ This umbrella comprises, among others, Statistical Analysis, Literature Reviews, Case Studies, and ‘Content Analysis’

(George, 2023). The only type that fits this thesis work is ‘Content Analysis’ due to the use of document sources (Romanosky et. al, 2019; George, 2023). Figure 5 illustrates the type and subtype of the qualitative research approach that fit the research work.

It is important to point out that the name ‘Content Analysis’ is just the name of a subtype of the qualitative ‘secondary research’ approach, and it should not be confused with the content analysis mentioned in later parts of this thesis as an activity conducted during the data analysis phase.

The practical implementation of the above-described qualitative research approach is divided into two steps: (a) data collection (see Subsection 3.3), and (b) data analysis (see Subsection 3.4). Figure 6 shows the two steps that are needed in deploying the qualitative research approach.

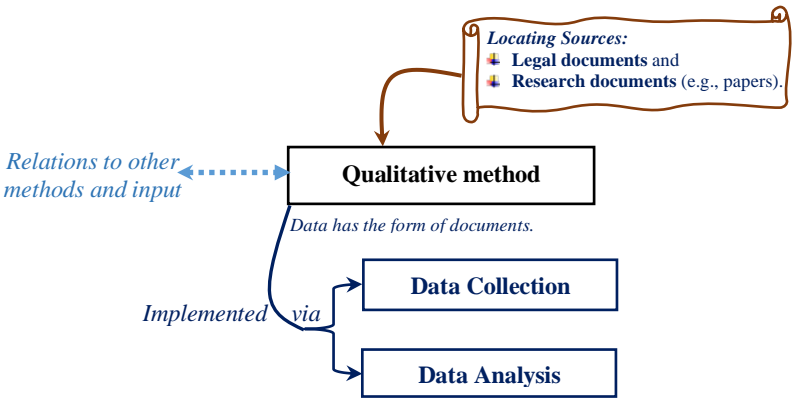


Figure 6. Implementation of the qualitative research approach via two steps: (a) data collection, and (b) data analysis. The data in this research is in the document form. Data collection is discussed in Subsection 3.3. Data analysis is discussed in Subsection 3.4. The relations to other methods and input links to the dogmatic method (e.g., result of interpreting a legal statement) and other technical input from the IT field (e.g., a related IT document that may come up in the future).

In implementing this qualitative research method, it is crucial to start by locating documents via choosing the accepted sources of data. Then the investigation can move to collecting documents that directly relate to the research questions. It is important to point out that in the rest of the work the investigation is done following the qualitative approach, while referral to the dogmatic method is only adopted when legal analysis, law hierarchy, or legal interpretation is needed at any stage. Moreover, after using the dogmatic approach, the corresponding result is carried back to the steps of the qualitative approach.

In this respect, after having located the documents, the data collection starts following a systematic way (see Subsection 3.3). Then the analysis step starts (see Subsection 3.4). In this step, the documents are thoroughly read with a mindset of investigating and analyzing them to answer the research questions.

When the investigation tackles legal documents, NIS2 is the main legal instrument to study. Due to the delimitations (discussed in Subsection 1.3), the NIS2

investigation should lead to a few selected articles to study. Studying the whole document needs larger volumes due to comprising 144 preamble constitutive paragraphs, 46 Articles, and several appendices. Moreover, locating a few articles based on a certain theme (e.g., finding and reporting InfoSec vulnerabilities) is good enough to serve the research aim of the thesis. It also aids in answering the research questions since it helps find a way to map legal provisions to InfoSec technical specifications. For instance, one possible technical specification could relate to relevant Common Vulnerabilities and Exposures (CVEs) and how to find and report them to the right technical database. Regarding the research documents (e.g., papers), rigorous readings are conducted to investigate their relevance based on the qualitative research approach.

All documents are evaluated and followed up on to see if any updates come up, especially for legal documents that can be updated, and amended. The major legal documents that are located (relevant to this research work) are presented in Section 3.2 on Sample Selection.

The analysis step leads to results. In the results phase, the obtained results will in turn- be investigated and analyzed to eventuate in a comprehensive mapping of provisions to InfoSec technical specs for healthcare CIs. In this way, SMEs can make use of the results to become more prepared in InfoSec especially that the work is mainly directed to EU SMEs as explained above in Subsection 2.1.7.

Looking at the thesis background (presented in Chapter 2), one sees that the research fields (InfoSec and law) are broad disciplines. Even though the technical implementations are not part of the focus of this research work, the overlap between the two disciplines includes some technical aspects. Therefore, it would support the research to look for available technical tools as well as develop a technical SW tool that aids SMEs to be compliant with some selected NIS2 article(s). One example for such a tool is a SW that can freely and quickly link certain NIS2 provision(s) to technical specs by finding vulnerabilities of SME assets as requested by the provisions. This example helps the reader relate the theoretical work of this thesis to the technical implementation i.e., it only serves as an aiding tool for the research. However, this tool may also be practically used by SMEs and any entity that desires to be compliant with the selected NIS2 provision(s).

In addition, this research revolves around two research questions (Section 1.2), which are “how” and “what” types of questions that fit the explanation by Crowe et al. (2011). The first research question inquires how to map selected articles of the NIS2 EU Directive to technical specifications for the healthcare sector in Sweden. One of the focal points of this study for healthcare CIs is collection of data from documents. This is because the interaction with healthcare CI individuals on a site in a continuous manner as described by Leedy and Ormrod (2015) is not possible for this study. This is a limitation, however, looking at this particular work with the aim of linking selected NIS2 articles to technical specifications, it can be done via investigating the documents that show the type of technology used in most healthcare CIs. For instance, by knowing that the Oracle Health component (as an asset) is used in abundance, the mapping from the legal text of NIS2 in relation to vulnerabilities can be made via immediate checks of CVEs related to this asset.

Another important issue to consider is that the findings could be difficult to generalize when following qualitative ‘Content Analysis’ as a subtype of ‘Secondary research.’ For instance, the process of mapping some NIS2 provision(s) on vulnerabilities to technical controls for electric power plants is different from the

process for a hospital. Therefore, one drawback is that in using this approach, one cannot be certain that it can be generalized to all cases. If generalizations are to be made, then they should be conducted in two ways, conceptually and analytically (Yin, 2013). The produced result should then be linked to existing literature, thus serving as an explanation for the gaps in this field, which is what this research work provides. In this regard, one shortcoming is that the research work may not be possible to generalize for all CIs according to Bell (2016).

A further issue to consider is that there is scarce work linking InfoSec provisions to technical specifications since most organizations are classically used to implementing standards. Moreover, having such laws to regulate InfoSec is relatively new. Due to this limitation and insufficiency of directly related work, the inductive reasoning is befitting. Observation is used to collect and filter data. Then the data is analyzed. According to Saunders et. al (2007), the last phase is to develop new links between laws and technical InfoSec specifications. Only one previous theoretical technique (IG 2.0) is found to be directly related to this study but is only found to fit specific cases. Hence, the work in this research starts by conducting observation in relation to reality, where the documents (including legal texts) are analyzed from the content viewpoint.

It is worth mentioning that the deductive approach is not considered since it relates to investigating an existing theory by deriving a hypothesis. According to the discussion by Saunders et. al (2007) on research methods for business, the hypothesis is- in turn- probed against empirical research. Such an approach is out of the scope of this thesis. One can argue that the study has some deductive parts, as the concepts gathered in the research background are likely to serve as a ground for deriving themes during coding.

Before discussing the two implementation steps of the qualitative research approach in detail, it is good to link this chapter to the background literature presented in Chapter 2 since a systematic literature review (SLR) is needed during the data collection step. It is the cornerstone for the rest of the work. Section 3.2 elaborates on the literature review to pave the way for the discussion on data collection in Section 3.3.

3.2 Sample selection: documents

Prior to discussing the Data Collection, it is vital to know what type of samples (sources) are needed to decide on the method to use in Data Selection. In this regard, the research is based on selecting documents since researching both disciplines (InfoSec and law) for mapping NIS2 legal text to InfoSec specifications for healthcare CIs depends on available documents. These documents are analyzed in the data analysis step. Part of the found documents are research papers, and others are legal documents provided by the EU and the Swedish authorities.

To focus the document selection on InfoSec for healthcare CI, NIS2 and MDR are chosen. This is because they are two relevant and powerful EU legal instruments that Member States can deploy to control the compliance of national organizations with InfoSec obligations in healthcare CIs. This compliance aids national governments in protecting EU healthcare entities and humans from possible security attacks. To further look at the Swedish perspective, the third document is the Swedish law on information security for socially important and digital services (SFS 2018:1174).

Based on the above-discussed sample selection, the primary subobjective is to ascertain whether information security regulative statements that relate to

healthcare CIs are mentioned in the legal documents. NIS2 is a network InfoSec legal document that relates to all types of networks i.e., CIs would be fitting, but a special look at healthcare networks is needed. Hence, its examination shall be processed in detail to better fathom the evaluation and follow-up procedures.

The MDR is an EU Regulation relating to medical issues, hence, not only does it have the highest level in the hierarchy, but it has an immediate and direct effect on control and compliance with any healthcare related organization in Sweden (and all other EU Member States). It includes accounts for specific situations and tasks that are declared as security incidents that need to be reported. However, they can conflict with the same cases in NIS2.

When specific InfoSec tasks are identified in such legal instruments to report to the concerned authorities, a thorough investigation of the content of these documents is needed. Other specific and general documents, papers, research documents, and reports may be included in the content analysis of the documents that relate to mapping regulative text to InfoSec specifications.

3.3 Data collection

Since interest in this research work aims at *understanding* the interpretation of selected NIS2 Articles and relating them to technical InfoSec specifications, then the most fitting data collection method is the qualitative one. Furthermore, the types of qualitative material to deal with comprises text, concepts, ideas, and figures. Therefore, the data collection method adopted in this thesis is 'Document studies,' where the execution of data collection is 'literature search.' Figure 7 illustrates the 'Document studies' method, literature review is considered as available data.

Papers and other kinds of documents are collected and analyzed based on a certain lens of study (which is part of the rigorous protocol i.e., to build a framework) looking at effectiveness, strength, and opportunities.

Therefore, the work in this thesis will apply the qualitative data collection method to summarize what has been done before, locate gaps, build on that to solve those gaps, and propose some solutions on how the related technology in InfoSec may be enhanced i.e., defining the features. The newly created knowledge is chosen based on being important and on creating value.

In this respect, there are various ways of conducting literature review. This thesis adopts the SLR as per the framework presented by Okoli (2015), which is discussed below in Subsection 3.3.1.

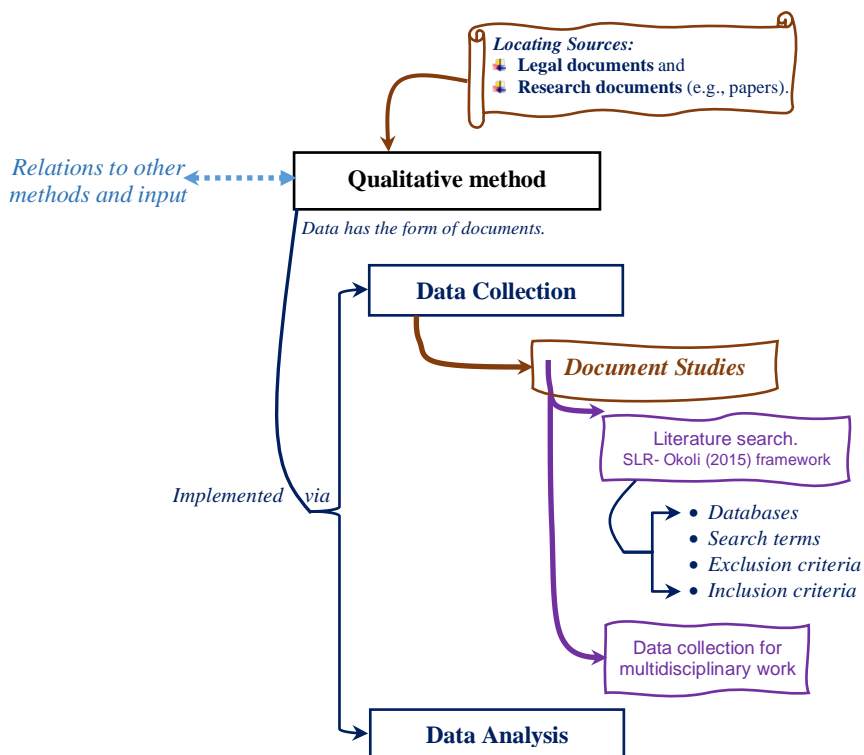


Figure 7. The data collection method in the qualitative approach is 'Document Studies.' The execution of data collection is 'literature search,' which follows the SLR of Okoli (2015) i.e., choosing databases, search terms, exclusion criteria, and inclusion criteria.

3.3.1 Systematic literature review (SLR)

SLR is very important for leveraging the quality of the research work since data collection is a cornerstone that depends on reliable literature review, and the whole research depends on it. According to Okoli and Schabram (2010), literature review for research purposes serves several goals including, among others, the theoretical foundation for further studies, fathoming the scope of research on a specific topic, and tackling practical and untillable questions via investigating published research.

It is worth mentioning that to render systematic literature review, three issues need to be thought of and chosen: (i) databases (see Subsection 3.3.2), (ii) search terms (see Subsection 3.3.3), and (iii) inclusion and exclusion criteria (see Subsection 3.3.4). Firstly, the chosen databases (e.g., IEEE, ACM) relate to the quality of selected documents and breadth of the document-search. It is vital for this type of thesis work to use peer-reviewed databases since the research questions deals with legal issues and their mapping to technical security parameters in a healthcare that is a life-critical field. Secondly, suitable, and topic-focused search-terms need to be identified relevant to the research questions. Otherwise,

the sample space of documents found may be too large to process. One technique to help in this issue is to have Boolean operators to enhance the search precision (e.g., NIS2 & InfoSec specifications). Thirdly, after the search the work subjects all papers and documents to inclusion and exclusion criteria, (which is a filtering process) to decide whether a paper/document stays as a source or not. The filter is decided before the search is started.

Common inclusion criteria are time spans (e.g., 2012), language (e.g., English, and Swedish due to Swedish laws), and being a 'peer reviewed' work.

Common exclusion criteria are duplicates (e.g., the same paper appearing in different databases), Lack of empirical results (no important insights and has no use), paid subscription. Accordingly, a 'relevance' indicator or a 'lack' indicator is added as a characteristic of the paper/document.

The choice of inclusion and exclusion criteria aids in filtering papers and files to eventuate only relevant documents.

Since the work adopts the framework presented by Okoli (2015), it is important to explain its eight (8) steps to conduct a systematic literature review:

1. The first step identifies the purpose of the review. The purpose is to locate relevant trustworthy sources that relate to mapping security legislation to technical controls and specifications while focusing on security for healthcare CI as the field of application, and Sweden as the nation where the results of the thesis would be used. This includes the subgoal of finding relevant legal sources for InfoSec and healthcare as well as references on the transformation of an EU Directive to a national law in Sweden. The motivation for this first step stems from the multidisciplinary nature of the research work.
2. The second step relates to drafting a protocol and training the team. It applies for reviews that include more than one reviewer. Such reviewers should come to complete agreement on the procedure they plan to follow. This requires a well written and detailed protocol document as well as training of all reviewers so that they execute their reviews in a consistent manner. This step does not apply to this thesis since it employs one reviewer.
3. The third step applies practical screening, which includes the elimination of sources. For instance, the review process eliminated sources such as national legislations that are not related to Sweden. All EU relevant legislations (on InfoSec and healthcare) are considered for review e.g., the MDR (2017), AI Act (2021), NIS (2018) and NIS2 (2020).
4. In the fourth step on literature search comprehensiveness, the following databases were searched: Scopus, IEEE Explore Digital Library, ACM Digital Library, and Science Direct. This search led to locating many papers, and the process also included inclusion and elimination of papers.
5. In the fifth step on extraction of data, applicable information from each source was identified and saved. This is done via thorough examination of the included sources and organization of the relevant materials, where the qualitative method is utilized.
6. In the sixth step on appraise quality, an internal score for reviewed sources is conducted to screen for exclusion, where the qualitative method is used also.

7. The seventh step comprises synthesizing studies (analysis), where the facts extracted from the studies are combined by using qualitative techniques.
8. The eighth step (final step) relates to writing the review based on the above description and the standard principles in writing research papers.

A note worth mentioning is that the papers are reviewed in the following way. Processing every paper starts by reading the abstract. If the abstract shows relation to the research questions and the aims, then the introduction is considered for reading. If the introduction reveals a motivation, problem, and solution related to the research, then the reading moves to the paper conclusion. If the conclusion shows relevant results, then a validity part is checked, and the paper discussion is read to come up with a summary about the paper and its relation to the research questions. Then the next step is to perform quality assessment i.e., when performing the filtering phase and a paper is fully read, the question would be to find if the quality is satisfactory or not, and if the paper relates to the research questions or not. Accordingly, a decision would be made on whether to include the paper, and which parts of the paper are considered in the research.

During the course of work, the literature review considered the database selection bias i.e., IEEE papers focused on technical aspects but not social aspects. This issue would not constitute a defect if the research method is aware of this bias since the work would use what is relevant from each paper/document. Moreover, the researcher bias is considered. Snowballing technique is also used in some papers when a paper is labeled as a good source, then the search moves to several references that are included in the paper. When the search related to legal papers and documents it was important to utilize the 'forward search' technique, where finding a relevant article that is newer was important. This is because in legal documents finding a fitting article/document in a certain year (e.g., 2019) may not be satisfactory since a newer article in a later year (e.g., 2020) may have updated legal information and changed laws or regulations. However, the good issue in this matter is that the newer article would be referring to the older one. This technique is used in several legal sources.

3.3.1.1 Databases

During literature review, locating papers and documents that relate to the research questions and aims is conducted over a set of source-databases that are popular for their quality and integrity. In particular, the main databases used for references are IEEE Explore, the ACM Digital Library, and ScienceDirect.

The IEEE Xplore is the digital library of the Institute of Electrical and Electronics Engineers (IEEE). It includes a very large database of peer-reviewed articles and a broad range of topics related to electrical and electronics technology. The topics include, among others, electronics, electrical engineering, computer science, biomedical engineering, information Security, Digital Health. It comprises journals, magazines, conference proceedings, and workshop papers. The focus for all documents in the IEEE database is of the research type.

The ACM Digital Library is the electronic library of the Association for Computing Machinery (ACM). Like the IEEE Xplore, it includes peer-reviewed journal

articles, conference proceedings, and workshop papers, besides other research documents.

ScienceDirect is a digital database for technical and scientific papers. Like the IEE and ACM libraries, it contains a large set of peer-reviewed journals articles, conference proceedings, and workshop papers. (Lancet, 2023).

Hence, the documents in all the above electronic databases are endowed with reliability, high quality, availability, and trustworthiness.

3.3.1.2 Search terms

Search Terms techniques aid the researcher to discover many related documents and articles that are needed for this thesis investigation (Jesson and Lacey, 2006). There are many documents related to Information Security in general, InfoSec legislations, and Critical Infrastructures. However, only a few documents combine the three topics, let alone adding the focal point of application to the case of healthcare Infrastructures. Hence, the main search terms used are "Security," combined with "law" or "legal" or "legislation" or "regulation" or "directive", combined with "NIS2" and "health" or "medical" and "Critical Infrastructure." These search terms proved very relevant and helpful for the search in this thesis. They are used to narrow down results in different operations and combinations. Oftentimes the logical operators "AND" and "OR" were used to concentrate on specific areas.

3.3.1.3 Exclusion and inclusion criteria

After choosing the search terms starts the filtering of documents by elimination based on relevance. Hence, an exclusion criterium and an inclusion criterium are best to utilize.

The inclusion criterium started by using the parameter of 'time span,' where any document from 2012 till the current date of the thesis is included. The next step was to include documents that are available based on the parameter of 'languages,' where a document is included whether it is written in English or Swedish (due to Swedish laws). The third parameter is the quality based on 'peer reviewed' work. However, since we trust the peer-review process in the above-mentioned databases, this parameter is taken care of by the choice of databases.

The exclusion criteria are based on the following parameters:

- Duplicates, where a document/article is excluded when appearing in different databases.
- Relevance and quality of empirical results, where an article is excluded if no valuable and utilizable insights are given.
- Type of source subscription where papers based on paid subscription are excluded.

It is worth mentioning that before the exclusion and inclusion criteria were employed, the search hits were many documents and papers. The inclusion and exclusion criteria ended with a set of labeled documents where each document is labeled with either 'include' or 'exclude.' Hence, the number of documents to consider as research sources was narrowed down to a smaller number that is manageable within the time frame of the thesis work including reviewing and analyses.

The search parameters for inclusion and exclusion were applied several times with different combinations. Table 1 shows detailed numbers of hits of the searches on all databases using the search strings and combinations.

Table 1. Hit and inclusion results based on search term combinations.

Search Term Combinations	Database Name	No. of Resulting Docs.	No. of Articles meeting pre-defined criteria	Most Relevant Docs.
"NIS2" and "Security specifications" AND "health"	IEEE Xplore	2033	32	3
	ACM Digital Library	730	28	2
	ScienceDirect	115	9	4
	Academia.edu	350	85	1
"Security" AND "Critical Infrastructures" AND Health"	IEEE Xplore	1003	100	4
	ACM Digital Library	263	30	2
	ScienceDirect	30	7	0
	Academia.edu	101	19	2
"Security" AND "Critical Infrastructures" AND specs"	IEEE Xplore	1160	15	5
	ACM Digital Library	3821	39	1
	ScienceDirect	90	3	1
	Academia.edu	376	22	1
"NIS2" AND "Medical"	IEEE Xplore	132	16	5
	ACM Digital Library	16	2	1
	ScienceDirect	7	2	0
	Academia.edu	69	1	1

The number of documents that met the predefined criteria is 410. Furthermore, thorough investigation and processes were rendered on those documents to choose the ones that can be most useful to this work, and the resulting most relevant were 33 documents with varying levels of utility for the research.

3.3.2 Data collection for multidisciplinary work

Data collection may use multiple sources especially when the research is multidisciplinary like in this thesis (InfoSec and law). In this respect, as the research in the Informatics field in this thesis follows the qualitative approach, part of the law-related material adopts the dogmatic method, which is often utilized in legal research. Shortly, the dogmatic method is important in this research since it provides the cornerstone for considering law hierarchy and since it sets standards for relating laws and dealing with the interface between different laws from the same level of hierarchy. This is needed, for instance, when NIS2 Articles are found to overlap with provisions from the MDR or AI Act in relation to the case of healthcare CIs. Since the work in thesis is directed towards an IT-reading audience, the Dogmatic method is briefly discussed at the end of this Chapter (see Section 3.7) so that the interested reader may refer to it if needed.

In this regard, qualitative techniques may be combined with other techniques, and this blending is referred to as data triangulation. The advantage of this mixing-approach allows the investigated issues to be observed from different angles. This provides a comprehensive view of the phenomena.

In addition, triangulation helps in confirming the research outcomes or questioning them. However, one issue to be careful about is that since data is viewed in two different ways, this may lead to confusion when the perspective of each

method leads to different outcomes. To tackle this issue, the research renders critical evaluation of the evidence to be of significance.

Another motivation for using triangulation is that it aids in leveraging the validity of the investigation (Yin, 2013) i.e., the fitting of the method is reinforced if the research questions are answered in a comprehensive manner (Bell 2016).

3.3.3 Collecting documents

Apart from the research articles and publications presented in Table 1 above, legal documents (EU and Swedish legislations) are collected. The EU legal instruments (e.g., NIS2 and MDR) are all available on the EUR-Lex³ website, which is an official site of the European Union. The Swedish laws and regulations (lag, förordningar, and SFS) are published and available on the website of the Swedish government site “Riksdagen.”⁴

For the legal instruments the research work considered the latest version of each of these documents while keeping track of changes with previous versions since it aids in document analysis. The legal documents considered are discussed in Subsection 2.1.7 and Section 3.2, and the major ones are two EU legal instruments (NIS2 and MDR), and one Swedish law (SFS 2018:1174).

The emphasis of the work is on NIS2 articles since it is the focal point of the research questions. Hence, only a set of its articles are considered. Several reports and papers were analyzed. One report was included (see Table 2), and the other documents were sixteen (16). The related research papers that were mostly read for research purposes are eight papers, which are shown in Table 3 (below) together with other sources. The total number of studied cases are twelve (12) and they are presented in EC (2023). Table 2 shows a sample of the main documents that are included.

3.4 Data analysis

As discussed in Subsection 3.3.5, in using triangulation, two methods are adopted when processing data collection. This enhanced the possibilities to grasp the research issues and the gaps after having located the problem (as described in the research questions). It also aids in enhancing the interpretation of the data that could result in seminal findings, especially that the dogmatic method allows the legal interpretation techniques discussed in Section 3.1, of which this analysis phase utilized extensive interpretation and analogies (induction and reduction). For more information about these legal interpretation approaches, which are permitted within the dogmatic method, the reader is advised to refer to Bernitz (2020). In brief, these interpretation techniques provide the basis for the golden rule of interpretation (Thombre, 2019), where the text is read word-by-word, investigated within the legal context and the case law (jurisprudence) to deconstruct the intended meaning in good faith and within social and ethical standards (within the EU and Sweden in this case). More importantly for this thesis, the use of the combination of this interpretation together with the qualitative method leads to data analysis procedures as discussed in the following subsections.

³ <https://eur-lex.europa.eu/>

⁴ <https://www.riksdagen.se/>

3.4.1 Qualitative content analysis of collected documents

The qualitative content analysis was conducted on a total of 9 legal instruments, three of which are EU legislations. The objective was to investigate whether follow-ups are needed and if they relate to the key words of the research questions i.e., InfoSec technical specifications, Critical Infrastructures, and healthcare. The content analysis method is an exploratory process. Hence, inductive, and deductive avenues are adopted in this process. Since the content in all the document records is qualitative, the content analysis is based on the approaches, methods, and techniques described above. Moreover, the criteria for inclusion and exclusion are always followed based on the specific search terms and term-combinations that express meaningful phrases from the research aims viewpoint. This is one of the main aspects of qualitative data (Saunders et. al, 2007).

The investigation conducted a content analysis of the legal documents, focusing on the clear content i.e., research-relevant content that is clearly expressed in the regulative provision texts. It is worth mentioning that only regulative provisions in the legal instruments are studied since the constitutive ones are out of the scope of this research, and this explains why the 144 preamble paragraphs of NIS2 were excluded from the content analysis. Another method used in this analysis phase is the IG 2.0 which showed some positive uses in particular types of legal provisions since IG 2.0 is mainly designed for institutional rules, that differ in aim, grammar, and intention from legal provisions as described in Chapters 1 and 2.

During the analysis phase, other documents, which are not legislative in nature, were also analyzed by looking at the content in a similar way. However, the difference was that the analysis was conducted without utilizing the legal interpretation techniques or the golden rule of interpretation. The first step in the content analysis was to go through each of the 16 documents to extract interesting (research-question relevant) data. This was also done using the keys (search terms) provided above in the inclusion and exclusion criteria. The search terms and consequent combinations of terms are shown in Tabel 1 (above). The outcome is then input in tables. An example of how the table looks like is shown in Table 3. The tables have four (4) columns, the first of which indicates the number of the studied documents in the research files, the way to refer to it (Reference), a short description, and the evaluation/relevance. Furthermore, some case law investigated relates to decisions that can be useful for future considerations in this direction. Hence, they are discussed briefly in Subsection 3.4.1.1 (below) so that the reader can get a rounded view of the research relevant documents for now and the future i.e., use as jurisprudence. Subsection 3.4.1.2 shows the outcome table.

3.4.1.3 Case law data

Inasmuch as the literature review search revealed in this regard, the cases C-62/19, C-194/94, C-194/94, C-144/16, C-62/19, C-275/19, C-390/18, C-299/17, C-320/16, C-434/15, C-255/16, and C-336/14 (2016) that are presented in EC (2023) are relevant to investigate- by analogy- for the scope and application of NIS2. This is because these cases, which are the only ones found so far as this search has revealed, relate to the applicability and scope of Directive (EU) 2015/1535 to lay down a procedure for the provision of information in the field of technical regulations as well as rules on Information Society services (EU,

2015). Studying these cases may aid in guiding Member State IT-representatives and industry in understanding the applicability of NIS2. The search for more case law will continue through the course of work in this thesis.

3.4.1.4 Main documents

This section shows in tabular form a summary of the main documents used and how they relate to the research work (see Table 2).

Table 2. Literature review summary in relation to the topic of the thesis research. The result is 36 documents of which 33 are from the results of the SLR part of the research presented in Table 1 (above).

Category	Reference	Short description	Evaluation or relevance
1	Zalnieriute et al. (2019)	The paper explores the tension between the regulations and the fast technological development concluding that automation can: (i) enhance it, and (ii) detract it from the rule of law values.	It aids this research in building upon its observations to evaluate whether automation of legal code translations would uphold the basic ideals of the rule of law when its outcome is a list of technical specifications.
2	Kianpour and Frantz (2021)	The paper analyzes institutional design of EU cyber incidents correctly considering the supranatural power of EU laws.	The paper constitutes a good basis for the high-level analysis part. It can also be used to take into consideration the supranatural nature of EU law when translating such high-level rules to the technical levels. It can be useful also to add the resulting technical specifications to be useful for crises management.
	Institutional Grammar 2.0 (Frantz and Siddiki, 2021; Frantz and Siddiki, 2022)	The work relates to encoding and analyzing institutional design. IG 2.0 specifies an integrated syntax for capturing information that is articulated in statements that are regulative and/or constitutive. IG 2.0 divides institutional statements into regulative and constitutive statements. IG 2.0 divides the text into basic units, where the unit of analysis is the instructional statement	Found possible and beneficial to apply for specific provisions only and in cases of regulatory statements but not constitutive ones e.g., few NIS2 articles like Art 11.
3	Creswell et al. (2016),	The paper articulates how characteristics of the qualitative method have several different ways to construct a mapping to technical controls/specs via capturing the meaning that the stakeholders need to follow.	Good for the section on Methodology. It can also partially aid in the way of interpreting the effect of the supranatural nature of the EU law
4	Thombre (2019)	This work explains the Golden rule of interpretation	Important for the interpretation of legal text.
5	Kowalski (1994)	This work tackles the problem of securing information via using several approaches e.g., IT system theory, computer science, sociology, criminology, and General System Theory to develop a model for socio-technical security systems for protecting information handled by IT.	Important for the socio-technical issues in the Discussion section. This model helps focus the analysis into four areas: ethics, politics and law, operations and management, and technology. All these areas are relevant to this thesis work, where the focus is on law.

6	Pasquale (2019)	This paper discusses the issue of legal automation, which is the field of using computer algorithms to automate the work of legal practitioners as well as trials of automating legal decisions. The author sees that success in legal analysis is only ensured by the success of persons in the legal field and not machines, yet.	Although legal automation is an interesting and probably promising field, the thesis work will not be considered useful for the investigation.
7	Carlson (2013)	The book elaborates the hierarchy of laws in Sweden, where EU law is the supranatural law.	Important for the discussion of transforming an EU Directive to a Swedish law
8	Riksdagen (2021a), Riksdagen (2021b), Riksdagen (2022a), Riksdagen (2022b), Regeringskansliet (2021), Regeringskansliet (2022), EC (2016), EC (2022a), and EC (2022b)	These references show how an EU legislation (e.g., EU Directive) is transformed into a Swedish law.	Important for the discussion of transforming an EU Directive to a Swedish law
9	Case law	Cases C-62/19, C-194/94, C-194/94, C-144/16, C-62/19, C-275/19, C-390/18, C-299/17, C-320/16, C-434/15, C-255/16, and C-336/14 (2016) that are presented in EC (2023)	Important for the discussion of transforming an EU Directive to a Swedish law
10	The ECA Review No 02/2019	The report found that the level of InfoSec preparedness was not enough.	Good to have to check the weaknesses in level of preparedness due to lack of linking legal texts to tech. requirements.
11	Otto and Antón (2007)	Literature Survey on addressing legal requirements in requirements engineering	Important to present the survey done on relating laws to technical specifications
12	NIS2	Main EU legal instrument	Very relevant
13	MDR	Supplementary EU legal instrument	Relevant for overlap with health-related issues and devices
14	SFS 2018:1174	Swedish law on information security for socially important and digital services (SFS 2018:1174), known in Swedish as "Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster." This law is the most related to NIS2, which is enforced in January 2023, thus it also needs to be transformed into a national law.	Article 1 (§1) SFS 2018:1174 deliberates the aim of the law and articulates the relevant fields that are divided into two categories: (1) socially important services in the sectors of "energy, transport, banking, financial market infrastructure, healthcare, supply and distribution of drinking water, and digital infrastructure," and (2) digital services (SFS, 2018:§1).

Several readings are required to contextualize the extracted sets in both the legal documents and other types of documents (including research articles/papers). Thus, categories were made based on the thematic coding approach. It is a structured approach for analysis of qualitative data. The essential idea is to find themes or categories in the data and summarize them. It often involves reading the data several times with different objectives. Two types of thematic coding can be used: (i) open thematic coding, and (ii) closed thematic coding.

In Open Thematic Coding, there are no pre-existing themes, and they normally come from a theory or previous literature. They are basically the concepts that

Figure 8 shows the exact location of the research focus (points 1 and 2) based on the time flow for NIS2, which is an essential point that falls within the aims and serves the objectives of the research questions.

3.5 Reliability and validity

It is vital for any research to be attentive to the risks that lead to doubting its validity based on the choice of method (Berndtsson et al., 2008). The research process is careful in considering the potential threats to the research choices.

It is worth mentioning that research validity refers to the intentions of two points: (i) what to measure, and (ii) how well these intended aspects are measured (Berndtsson et al. 2008). As mentioned earlier in Chapter 2, the previous work on the area of mapping legal texts to technical specifications (especially for InfoSec in healthcare CIs) has scarce relevant work and knowledge. Hence, the evaluation and follow-up responsibility from NIS2 as an EU Directive to become a Swedish law that can be interpreted in a way to transform some of its provisions into InfoSec specifications would be difficult if the choice of the research method was not qualitative. Moreover, the specific approach is that of Secondary research, as described in Section 3.2. In addition, the type within this method is 'Content Analysis,' which utilizes reliable existing documents as data sources (George, 2023).

In data collection, text material like papers, white papers, books, legal instruments, and other types of reference material are read as primary documents to be used in a new (secondary) research study fitting the qualitative type of 'Content Analysis' (George 2023). The work uses the inductive approach and is proven appropriate since the results were shown to be repeatable and meaningful (See Chapter 4).

When conducting the 'Content Analysis' type of the qualitative methodology, the researcher must fathom the problem in advance. The researcher may also have chosen a case study to advocate some points (Yin 2009). However, in this thesis, the case study is for a whole industry (that of healthcare), which is verifiable according to Yin (2009). Nonetheless, much of this work remains under 'Content Analysis' since it deals with documents only. Therefore, a risk and threat to the reliability of this qualitative research is researcher bias.

When conducting a 'Content Analysis' for a whole industry (case of healthcare), the researcher may have already set concepts. Thus, any bias should be noticed and reported by the researcher (Berndtsson et al. 2008). A researcher with an interest in the phenomena under investigation may suffer the risk of bias. To face this problem, this thesis work is aware of this issue and considers all data with equal attention. Hence, the risk is minimized as described by Bell (2016). To avoid such a bias, the literature review is extensive to not miss any vital aspects. Moreover, the analysis is thoroughly done and objective so that the outcomes are valid and reliable.

The selected legal documents are the final resort to potential reliability issues. In other documents, it is important to consider that the author may have published them with bias (Bell 2016) unlike the legal instruments.

3.6 Ethical considerations

Most studies adopting the ‘content analysis’ type of qualitative research deal with real life topics, hence, ethical considerations are crucial (Yin 2009). There are three main ethical requirements to consider.

Firstly, the researcher should clarify and clearly articulate the purpose of the study via research questions.

Secondly, integrity in copying laws and legal text is important. This is because most readers of this work are technical people, and they may not refer to the legal documents to make sure that the copied legal provision or the interpreted ones are exactly as the researcher is claiming. Hence, it is the job of the researcher to ensure integrity.

Thirdly, collected documents should only be used for research purposes (Patel and Davidson 2019).

The thesis seriously considers all these requirements.

3.7 The dogmatic method for legal sources

The dogmatic research method, also referred to as the doctrinal method, is oftentimes used in legal research since it concerns researching law, international legislations, legal principles, legal concepts, doctrines, case law and legal literature (Smits, 2017). The sources are mainly related to legal processes including inter alia principal statutes, regulations, legal literature (e.g., papers and books), court cases, and arbitration cases (McCrudden, 2006). The parts of the thesis investigation that relate to legal analysis, hierarchy of laws, and legal interpretation techniques adopt the dogmatic method’s main goals of describing, prescribing, and justifying a thesis.

The dogmatic method is referred to in this thesis work only few times during the data collection and analysis steps, and that occurs when a phrase, statement, or document has a legal aspect that needs to be investigated and analyzed in a legal manner i.e., legal methods and techniques are required to render the investigation. This method helps the data collection and analysis steps of this work via allowing for a methodical discourse of laws, directives, doctrines, regulations, rules, legal interpretation, and other legal issues related to the two other disciplines of Informatics and healthcare. One example lies in relating legal codes to InfoSec technical controls in a hospital environment (i.e., CI) in Sweden that utilizes an Oracle Health asset. Appendix 1 shows a detected InfoSec vulnerability in such a case, where the detection is based on linking Article 21 NIS2 to technical controls. Moreover, this can only be detected by following the above-described interchange of the two research methods, qualitative and dogmatic.

Moreover, the dogmatic method leverages the investigations via locating, identifying, and clarifying legal problems and uncertainties. This is accomplished by analyzing relations between legal sources e.g., the abovementioned overlap between the NIS2 Directive and the MDR as well as the Swedish legal instruments (e.g., SFS 2022:508).⁵ It supports investigating the divergence/convergence of several legislations when they overlap in one application such as healthcare CI

⁵ Figure 8 shows the SFS location within the process of linking a Swedish law to EU legislations. It aids the reads to see the link between EU legal instruments and the Swedish one (SFS) i.e., the overlap exists but the problem of the overlap leads to conflicting requirements.

security in Sweden (see paras 9 and 10 in Section 1.1 on the overlap discussion between NIS2 and the MDR).

In addition, the dogmatic method implementation in this thesis makes possible the treatment of the topic of mapping legal articles (e.g., NIS2 articles) to technical controls/specs and their legal practice as one ordered-set e.g., a set of codes in one legal instrument (Smits, 2017).

An intriguing issue in the dogmatic method for this work is that it aids in systemizing and adapting regulations to modern realities e.g., systematically interpreting the NIS2 Directive that needs to be accommodated as a national law, considering recent legislation revisions, and analyzing legal practice and case law in relation to social changes (Smits, 2017). For instance, there have been changes in security demands and practices after the increase in cybersecurity attacks on healthcare systems and medical devices during the Coronavirus pandemic (Ceruleus, 2020; Schwartz, 2020). Furthermore, demands for change increase as healthcare gets more digitalized, because digitization of medical devices and systems adds more security risks (Lekshmi, 2022).

The thesis employs the dogmatic method to investigate selected Articles of the NIS2 Directive via: (i) investigating how specific definitions like CI and 'essential' entities' affect the opponent and proponent arguments on the mapping to specific technical controls (with consequent challenges), (ii) locating legal bases for technical specs, and (iii) analyzing several legislations at the same time.

In implementing the dogmatic method, the thesis adopts the framework articulated by Hutchinson and Duncan (2012). This framework comprises seven (7) steps of the dogmatic method (presented below). It is worth noting that every time the investigation refers to the dogmatic method, the below 7 steps are followed (Hutchinson and Duncan, 2012):

1. The first step relates to 'assembling relevant facts.' Hence, it starts with understanding the area of investigation and at which point of the investigation would the legal issues be considered. This is important to decide on what facts can affect the following legal analysis. For instance, the existence of healthcare concerns, laws, and policies is a fact that must always be included at this step. Moreover, the existence of legal obligations in two different laws that conflict regarding a certain application would be considered as a fact. This is sensed from the first step when dealing with NIS2 and the MDR. Then, this step requires setting a proposition as the starting point. A sample proposition may consider linking articles from NIS2 and MDR e.g., Article 20(4)(a) NIS2 and Article 87(3) MDR. These legal provisions would now be in question, or the existing laws could be chosen for the purpose of the thesis. The next issue to render in this step could be to analyze the purpose behind bringing particular law(s). For example, for a provision of the NIS2, a related MDR article could give great and valuable insight.
2. The second step deals with 'identifying the legal issues' to study. For instance, after referral to the dogmatic method while studying a certain source/document, and after facts around the document are gathered, it is pivotal to decide whether there are any legal issues of concern (e.g., unclear, or controversial issues) related to this document e.g., a certain phrase/statement that is creating a conflict or requires interpretation. In this respect, a major task is reviewing the NIS2 Directive to identify

issues related to healthcare security in Sweden to be able to link them, at a later stage, to InfoSec technical specs.

3. The third step relates to ‘analyzing the issues with a view to search for the law.’ These issues are the ones determined above in the second step. For instance, the thesis uses IG 2.0 to investigate if it could be applied to the legal issue (deconstructing the legal code to solve the issue at hand). Hence, this step includes a possible breakdown of legal articles.
4. The fourth step focuses on ‘reading background material’ that aids in resolving the legal issues located in step 3. In this regard, the dogmatic method allows referring to secondary legal sources e.g., articles, reports, and books. For instance, in the thesis work, when investigating Article 21 NIS2, some legal issues were located as per step 3 (above), where conflicts of laws were found with MDR Articles. To resolve this issue the investigation had to refer to secondary legal sources like legal dictionaries, law textbooks, legal encyclopedias, law and policy papers, and journal articles.
5. The fifth step works towards ‘locating primary material’ comprising legislation, directives, delegated legislation, regulations, and case law. What is interesting in this step is that it oftentimes comes after some secondary resource is being read and this source is found to refer to a primary legal instrument. This step is very helpful in the thesis work since it used the work and effort of step 4 to locate relevant laws that may relate to (or conflict) with NIS2 like the MDR and other Swedish laws.
6. The sixth step involves ‘synthesizing all the issues in context.’ This comprises breaking down each studied legal provision (e.g., NIS2 article) to several obligations. It uses the results of the three previous steps to transform the recognized obligations/objectives to technical controls.
7. The seventh (7) and final step relates to ‘coming to a tentative conclusion.’ It tries to validate the results of step 6 e.g., to have legal compliance with the NIS2 Directive selected article without diverging from other requirements of other relevant legal instruments (e.g., MDR).

4. Results

The abovementioned research methods (see Chapter 3) allow the data and studies to be collected and documented from various resources e.g., governmental records, business organizations, scientific papers, articles, legal dictionaries, EU website, books, and digital libraries. These sources are categorized into primary data (collected in the investigation) and secondary data (from other sources).

After data collection and analysis, the research leads to a thorough review of the NIS2 Directive Articles that is relevant to healthcare security implementation in Sweden.

A further result is a combination of interpretation methods to encompass the new InfoSec realities provided by NIS2 to ensure that the technical specifications are flexible and viable enough in the foreseeable future. Hence, the results include what is needed in the Healthcare sector from the viewpoint of NIS2.

A third result related to guidelines for the Healthcare sector in Sweden on overlap with other legislation would be presented.

This work can lead to a set of identified actors/actions that could be used to exploit vulnerabilities in healthcare systems in Sweden. Furthermore, some compliance frameworks may be found e.g., ISO 27001, NIST Cybersecurity Framework, SOC 2, and more.

One important result is a final mapping table between the NIS 2 selected Articles and several technical specifications that can be applied to healthcare (as CI) in Sweden with legal and technical explanations on the choices made. It is also important to keep in mind that compliance with the NIS2 Directive should be an ongoing process, so a relevant result is to build the tables so that organizations can regularly review and update its compliance measures and technical controls/specs especially when relevant legislations are revised, or new legislations are published. This is necessary to ensure that the resulting mapping tables remain in line with the latest legal obligations.

4.1 Information security definition

Spotting the relevant legal definition before conducting research is vital, because it lays the bedrock for investigation. There is no common definition for InfoSec that is accepted by all public and private entities and organizations (Horne et. al, 2016). Article 6 NIS2 includes the definitions for various terms, but it does not provide a definition for the exact term ‘information security.’ Related phrases in Article 6 include: ‘security of network and information systems,’ ‘cybersecurity,’ and ‘national cybersecurity strategy.’

This adds to the confusion since InfoSec relates to the multidisciplinary work in this thesis (InfoSec and Law). The thesis tackled this issue in Subsection 2.1.3 (InfoSec in the Context of Research Scope) via adopting the concept of InfoSec discussed by the ISO/IEC 27000:2018 standard that defines InfoSec as the “preservation of confidentiality, integrity and availability” (CIA) of information (ISO, 2018:3.28). An issue to further consider is whether this adoption would go in harmony with NIS2. In this regard, NIS2 para 79 (in the preambles in NIS2) mentions ISO/IEC 27000 series as a standard that it recognizes. An opponent to this definition may argue that NIS2 did not particularly link its understanding of InfoSec to the ISO/IEC 27000 family of standards.

However, the proponent investigating this issue within the scope of this thesis work interprets NIS2 para 79 via utilizing the “purpose interpretation” method, which looks at the provision from the perspective of the intention and general purpose, especially that this interpretation method oftentimes is used in legal matters to compare texts with EU preambles (Bernitz, 2020). Thus, it can be construed as NIS2 refers and adopts what is presented in the ISO/IEC 27000 family, because the InfoSec definition in ISO/IEC 27000:2018 is a corner stone for the points in the ISO/IEC 27000 series that NIS2 accepts.

4.2 Socio-technical aspects

IT systems in general have always suffered from the problem of InfoSec and the possible attacks on IT assets. This IT insecurity issue is formulated in Kowalski (1994) as a property of socio-technical systems at four levels: international, national, organizational, and group-individual level (see Figure 3).

In relation to this thesis work, international (EU) sources and national (Swedish) sources are considered. NIS2 is an EU directive i.e., it is an international legal instrument as discussed in Chapter 2 (Background). The Swedish laws like SFS (2022:508) are national legal instruments. The flow of effects of an EU directive like NIS2 starts by forming obligations on nations to produce local (national) laws. This is related to the flow of processes shown above in Figure 8. However, these nations (e.g., Sweden as an EU Member State) have their own societal considerations, ethical values, and norms, which are reflected in their legislations. Therefore, in transforming an EU directive like NIS2 from an international EU level to a national law, there are staunch links between the social considerations, legal constitutive and regulative provisions, and technical specifications (e.g., InfoSec specifications). Hence, one result in this direction is that this study has a socio-technical element that can benefit from socio-technical studies and research (see Subsection 2.2.5).

Another sub-result is that the flow of effects from an international level (e.g., EU) to a national one (e.g., Sweden) continues to affect organizations (e.g., SMEs), CIs, and individuals. Figure 3 provides a visual illustration of this top-down flow. In the legal field, such an effect (from EU legislation to a national one) is referred to as direct effect (Bernitz, 2022). Hence, NIS2 has a direct effect on national and organizational system levels.

Considering the system provided by Kowalski (1994) and shown above in Figure 3, the result is that the focal points of study (points 1 and 2 in Figure 8 presented in Chapter 3) are linked to this flow. Point 1 is where EU legislation is enforced, and in the case of NIS2, it is a directive that flows to the national government with the responsibility to process and transform it to a national law as per the flow shown in Figure 8. Hence, Figure 3 and Figure 8 are related on the international and national levels. Point 1 on Figure 8 is on an equidistant range from the International system level and the National system level in Figure 3, and point 2 is between the National system level and the Organizational system level in Figure 3. Hence, the studies and theories published in relation to this flow in Kowalski (1994) apply to this work. This is a door opener for further development and future work on NIS2 in this regard, for any EU Member State.

These are important results since a number of factors can lead to disequilibrium in the socio-technical system (Kowalski, 1994). On the other hand, Kowalski, (1994) discusses several measures that can be taken to correct it and keep it in

equilibrium. Examples of measures in Kowalski (1994) are having computer virus protection on the organizational level and laws on the national level that can affect the probability of virus programs being written and distributed. The thesis looks further on the international level (EU directive) and its effect on the lower levels shown in Figure 3 especially the national one, where not only the Swedish government is concerned but also organizations, SMEs and other public sector entities.

However, the thesis uses the distinctive separation on the national level as per the one in Figure 3 i.e., via looking at the organizations being on a lower socio-technical level than that of the nation. This result is very important since it goes in harmony with the hierarchy of laws discussed earlier in Subsection 2.1.5. This is needed since the thesis work needs to be applicable and reliable, otherwise SMEs would not benefit from using any of the results including the developed computer tool (presented below in Section 4.4). To be applicable and utilizable without considering the separation between international, national, and organizational levels, the hierarchy of laws would not match the research and the results would not be reliable due to mixing up levels of legal authorities (legal instrument authorities e.g., EU law) thus creating undesired confusion. Therefore, a valuable result is that the hierarchy of laws that is supported by the dogmatic method is applicable within the socio-technical framework shown in Figure 3 and discussed thoroughly in Kowalski (1994). Accordingly, the effect flows from the EU directive (NIS2) to the national level (Swedish law), then to organizational rules and InfoSec technical specifications that comply with the national law. The national law- in turn- must comply with NIS2. Thus, no conflicts between legal, social, or technical parameters exist when this is adopted. Moreover, all the results of Kowalski (1994) on InfoSec in relation to socio-technical considerations are applicable. They also can fall in handy for deployment in real scenarios within the answers to the research questions of this thesis.

A third interesting sub-result relates to the implementation gap that exists after a legal instrument is issued and the administrative/managerial layer needs to transform it to the level of operation. According to Kowalski (1994), administrative and managerial layers are supposed to find requirements then implement and test them. Nonetheless, Kowalski (1994) argues that oftentimes they are stuck in a loop between principles and policy. This is illustrated in Figure 9 (see red brace in Figure 9 to notice the loop). Hence, it is hard to move to the requirements phase, which can sometimes be due to a lack of interpretation or understanding of the policies, rules, or laws (Kowalski, 1994). The thesis work helps move out of the loop to the requirements phase. Moreover, according to Kowalski (1994) the implementation and testing phases are not well processed and confused, where usually one finds that running tests occurs even without any implementation of any specification. This gap is seriously dangerous especially in the field of InfoSec since technical requirements and specifications need to be well studied and presented to the operation layer. Figure 9 shows these issues and provides a visual representation of the links between the different layers in a top-down approach. It flows from the ethical layer to the legal layer, then to the administrative/managerial one, then to the operational one (with a big question mark), and finally to the technical operating system.

Looking at the gap representation in Figure 9 (pointed to by the blue arrow), the reader can notice that the managerial groups may start the testing of some work without having thoroughly understood the legal instrument or worked on its requirements and implementation.

In this regard, the thesis partially contributes to showing the method to solve this issue for NIS2, and the computer program tool (presented below in Section 4.4) also serves in the implementation phase since it can aid the management to locate vulnerabilities automatically, and the operational team would know what to look for with clearer plan. The tool also partially serves the testing phase since it has already dealt with few NIS2 articles, and it was run on few healthcare assets in CIs. So far, the testing showed good proof of concept. However, this is partial testing, and it is only for a small part of what needs to be tested in InfoSec in relation to NIS2. Nonetheless it is a start and a door opener for further development in this avenue for NIS2 compliance.

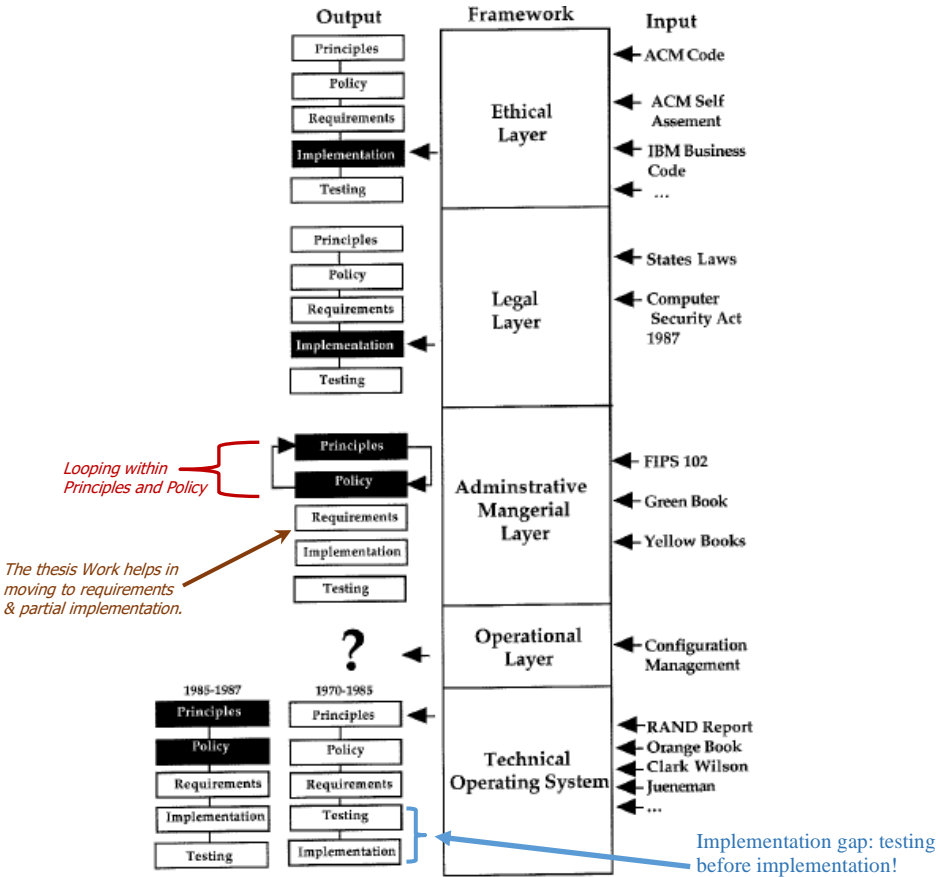


Figure 9. Combined static and process meta model (Kowalski, 1994:fig.11.5). Permission to use this figure in this thesis is granted by the author of Kowalski, (1994). The red brace shows the area where administrative and managerial personnel can be stuck in a loop between principles and policy i.e., never existing the loop to specify requirements, which is what the thesis contributes with (see the brown arrow). The pre-implementation gap is pointed to by the blue arrow.

A fourth sub-result is that, considering the ‘question mark’ area in Figure 9, points 1 and 2 in Figure 8 would correlate with the operational layer and the pre-implementation gap shown in Figure 9 as well. This is very important for the research study and the proposed computer tool. In this regard, the EU directive lies in the pre-implementation gap in Figure 9, which is where point 1 lies in Figure 8. When an SFS (Swedish legislation) is considered as well, point 2 in Figure 8 would logically link to the pre-implementation gap (blue arrow in Figure 9).

This means that when using socio-technical measures for the NIS2 implementation, the choices shall be regarding points 1 and 2 in Figure 8. Using the details of Figure 8 can leverage the quality, reliability, and validity of the results since the figure shows how to relate and use them in real cases like court cases, doctrines, and within Swedish legal bodies.

4.3 IG for selected NIS2 provisions

Institutional Grammar (IG) 2.0 as detailed in Frantz and Siddiki (2022) is discussed in detail in Subsection 2.2.2. As the name indicates, it is a technique created to aid in understanding requirements from institutional texts including institutional statements i.e., having a professional purpose.

One result in this regard is in relation to trying to use IG 2.0 for legal text (e.g., NIS2 articles). Firstly, IG 2.0 has not been proven to function for legal text and this is still a big question that IG 2.0 researchers are trying to investigate. However, it seems to be a long way before one can get an answer on that. This brings the discussion to the second point, which is what this thesis contributes with in relation to IG 2.0 and its use with NIS2. The investigation looks at many NIS2 articles and it focuses on articles that relate to two main legal topics of high value for NIS2 and the EU:

- (i) InfoSec vulnerabilities discovery.
- (ii) vulnerability disclosure and reporting rules; where the study investigated the applicability of IG 2.0 to NIS2 Articles 7(2)(c) which refers to Article 12(1), Articles 11(3)(a), 11(3)(b) & 11(3)(e), Articles 12(1)c, 12(2), 12(2)(c), and 21 with special attention to 21(2)(e).

As discussed in Subsection 2.2.2, IG 2.0 is designed to deconstruct two types of statements: regulative and constitutive. Regulative statements are similar (but not identical) to law provisions (e.g., NIS2 articles). They articulate a description of actions related to specific actors with certain contextual parameters. So, when checking the deconstruction of a NIS2 article, the research looks at the following distinctive parameters: attribute, aim, context, object, deontic, and an ‘Or else.’ These are described in Section 2.2.2.

Constitutive statements constitute or parameterize characteristics of a system, hence they may (in some cases) fit analyzing the preamble paragraphs in NIS2. These statements are not used since the work looks at NIS2 articles.

When interpreting NIS2 articles with IG 2.0 it is sometimes too complicated, and IG2.0 misses some parameters to represent all the legal text. When the legal article is too long and inter-linked with preambles, other laws, other provisions, and sometimes societal and ethical aspects, then using IG 2.0 is not a sure avenue to go through since the results may not be reliable, reusable, or even reproducible for InfoSec specifications.

This section takes one example to an article in NIS2, where applying IG2.0 to the whole article is more time consuming than using any of the legal interpretation methods (see Appendix 3) but it applies IG 2.0 to a part of this article.

From a legal compliance viewpoint, one of the most relevant and important articles within the thesis scope is Article 21 NIS2 'Cybersecurity risk-management measures' (see Appendix 4). However, when using IG 2.0 for this article, the first problem facing the technique is the length of the article. Other problems include the intricacy and links from other articles to it. For instance, reading Article 21 alone would not be sufficient without having read Article 20 'Governance' before it especially that Article 20(1) refers to Article 21. Such pre-links that need to read the document/source (legal instrument) as a whole, are not possible to take care of with only IG 2.0. This is one reason why IG 2.0 needs to be combined with other techniques and interpretation methods to give the right meaning that can lead to the right InfoSec specifications. This is one important result.

Nonetheless, another result for using IG 2.0 that this thesis contributes with is that the researcher can take a part of the article and apply IG 2.0 to it. This is possible in this research work since it focuses on answering the research questions on how to transform the selected article(s) in the context of healthcare CIs, where vulnerabilities are vital. So, by focusing on such vulnerabilities, the thesis shows below how it is possible to use IG 2.0 for a small statement within the legal Article.

The thesis chooses the most relevant part of Article 21 in relation to the scope, which is Article 21(2)(e). However, it cannot stand alone, when using IG 2.0. So, to be able to utilize IG 2.0, the researcher needs to take the main statement in Article 21(2) and add option (e) to it to formulate a statement that would look to the IG 2.0 user as being similar to an institutional statement.

Hence, this result means that the researcher needs to process the following algorithm:

- (i) divide the legal article into several statements and phrases.
- (ii) choose the statements of interest.
- (iii) add the sub-statements in step (ii) together to form a full statement that includes some of the parameters of a regulative institutional statement.
- (iv) check if the new statement refers to other paragraphs within the article.
 - o If yes, add the referred-to article.
 - o Else, move to step (v)
- (v) apply the IG 2.0 separations on the statement to locate the parameters.
- (vi) analyze

In applying the above algorithm steps (i) to (iii), with the focus on the issue of InfoSec vulnerabilities, then the following can be truncated and appended from Article 21:

Article 21(2) NIS2

"2. The measures referred to in **paragraph 1** shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

...

(e) security in network and information systems acquisition, development and maintenance, including **vulnerability handling** and **disclosure**.

...

However, in applying step (iv) on checking the condition of referral to other paragraphs, it is clear that para 2 refers to para 1. Hence, a thorough look at para 1 is needed (see Appendix 4). Paragraph 1 refers to ‘all-hazards approach,’ which is a comprehensive emergency preparedness framework that considers the full scope of emergencies and disasters during the response and mitigation planning (AlertMedia, 2023). Hence, investigating Article 21(1) shows that we can assume for the purpose of this thesis to neglect it for now, and try to add the IG 2.0 regulative statement parameters to the above statement. The result is as follows;

<i>Attribute</i>	<i>Deontic</i>	<i>Aim</i>
<i><u>“The measures referred to in paragraph 1</u></i>	<i><u>shall</u></i>	<i>be based on</i>

Object

an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following (Context):

...

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

...

In applying step (v) the analysis again needs a legal interpretation method, so IG 2.0 is not enough alone. Using the linguistic and End Goal interpretation methods combined (see Appendix 3), the researcher construes the statement to mean that InfoSec vulnerabilities must be: (a) handled, and (b) disclosed.

IG 2.0 was only helpful when used with other legal interpretation methods, but it cannot be used alone. Moreover, to construe the full meaning to relate it to technical specifications, the End Goal interpretation method needs to be applied, and when doing so, a reading of further articles (indicated above) is done. Processing all these articles would lead to the final interpretation that when a CI has InfoSec assets, it should discover vulnerabilities to be prepared within EU protection needs, then it needs to handle these vulnerabilities and disclose them.

Handling may take longer time so disclosure and there could be an overlap in case the handling was not successful. This calls for amending this interpretation to look at Articles where reporting vulnerabilities is mentioned. This reporting is the action taken to disclose the located vulnerabilities to the right authorities based on NIS2. It is worth mentioning that, according to NIS2, the final destination for reporting is an EU database to be established by the EU authorities.

Therefore, the issue of timing of disclosures and reporting of vulnerabilities and incidents becomes vital to investigate. This thesis tackles this issue of disclosure-timing and finds out that it not only depends on NIS2 but also the legal documents that relate to the field of application e.g., healthcare in this case. Section 4.5 discusses the results on the overlap of NIS2 with other laws regarding the timing issue and shows that when an incident occurs then timing differences between different laws (of the same hierarchy as being EU legislations as NIS2 and MDR) can overlap over incident reporting and have different timing schemes.

Section 4.6 discusses how to map this timing issue to a technical specification, which is one of the goals of this thesis.

However, before moving to timing issues and interfacing between laws, it is good to mention that for the sake of aiding the research and SMEs in fast and reliable implementation for the NIS2 requirement to find vulnerabilities and disclose them, a computer program tool can support the work. This tool is developed during the research work, and it is discussed below in Section 4.4.

4.4 Tool for vulnerability discovery and disclosure: NIS2 compliance

Many open-source and commercial tools exist for vulnerability discovery (Tyani, 2023). Examples include, among others, Zenmap (Lyon, 2017), Nessus (Cranenburgh and Garcia-Alfaro, 2019), and Nexpose (Sharma and Nagpal, 2017).

However, the advantage of the tool developed in this thesis is that it is free for SMEs, its algorithm is fast, and most importantly it is written with the aim to comply with NIS2 and is optimized for checking vulnerabilities related to health components and devices. Hence, it is more fitting for any entity (private or public) that needs to check vulnerabilities per the NIS2 requirements for healthcare CIs. It is a tool that takes the legal perspective and changes that to technical parameters.

Within the course of research, it was clear that a computer program (as a digital tool) would aid in supporting the results of the thesis as well as showing reliability and repeatability of some of the results.

The tool can take an input from the user regarding the field of interest, which is 'health' in this thesis, and accordingly searches CVEs that are reported. It renders a thorough check on any possible matches to provide the user with a list of matching CVEs, based on the CVE Identification (ID) number to the asset (IT component) under investigation.

Up to the knowledge in this thesis work no other available tool than the one provided by this research can relate the field vulnerabilities (the field is 'health' in this case) to common technical errors that occur due to InfoSec attacks.

One example of how the tool works in relation to compliance with NIS2 is via the implementation of the technical checks needed to comply with Article 21 NIS2. This article requires finding vulnerabilities of the assets in an organization. Hence, the tool takes, as input, a Comma-Separated Values (CSV) file that contains the names of the models of the assets e.g., a type of Oracle Healthcare component. Accordingly, the tool checks every component (asset) that is listed in the user CSV file against CVEs (vulnerabilities) that are publicly available in CVE records in databases from the year 2002 till 2023 (Mitre, 2023). Once a match is found, it is saved in an output CSV file, which lists the asset number in the organization together with the related vulnerabilities.

Accordingly, this CSV output file forms the basis for the vulnerability checks as required by Article 21 NIS2. It is a technical result with a technical specification that relates to a legal requirement of vulnerability discovery in NIS2. The CSV output file can then be disclosed and sent to the related EU CVE Record Database as required by NIS2.

The tool code was made with Python and run on the following specs:

- Processor: Intel(R) Core(TM) i5-1035G1 CPU@1.00GHz, 1.19 GHz.
- Installed RAM: 8,00 GB (7,79 GB usable).
- System type: 64-bit operating system, x64-based processor.
- Edition: Windows 10 Home.
- Version: 22H2.
- OS build: 19045.2846.
- Experience: Windows Feature Experience Pack 120.2212.4190.0.

The average time that the Python tool consumes to render the results is around one (1) minute.

Appendix 1 shows a sample of one of the vulnerabilities found by the tool, where there is a matching between the organizational asset and the CVE in relation to a healthcare component in the organization. The asset belongs to the Oracle Health Sciences InForm products of Oracle Health Sciences Applications.

Figure 10 shows a sample output for matching vulnerabilities per the requirements of Article 21 NIS2 (NIS2 compliance) via printing the unique vulnerability identifying number (CVE ID) for each asset.

```
$ python search_vul.py
Processing JSON file: nvdCVE-1.1-2020.json
Asset 1 Version _15.0.1_ is vulnerable based on CVE whose ID is: CVE-2020-1455
Processing JSON file: api/json/nvdCVE-1.1-2021.json
Asset 2 Version _15.0_ is vulnerable based on CVE whose ID is: CVE-2021-31827
Asset 3 Version _15.0.1_ is vulnerable based on CVE whose ID is: CVE-2021-33894
Asset 4 Version _15.0_ is vulnerable based on CVE whose ID is: CVE-2021-38159
```

Figure 10. Tool output on matching vulnerabilities as per the requirements of Article 21 NIS2 (compliance)

Appendix 2 shows sample outputs of the tool and explains them briefly. An interesting aspect of this output is that it shows how the tool can relate several technical errors that occur due to InfoSec attacks that abuse the already matching CVEs.

For instance, Appendix 2 shows the result of relating a 'health' component (asset) in an organization to possible technical errors that can occur when the matching CVEs to this asset are abused. The technical errors used in this example are Overflow, DoS (Denial of Service), XSS (Cross-Site Scripting), SQL injection, and Memory corruption. Descriptions of these technical errors and their relationships to vulnerabilities are described in Appendix 2.

The time that the Python tool took to render the relationships between the technical errors and CVEs matching the asset was fifty five (55) seconds.

Figure shows the tool with its output relating to Appendix 2.

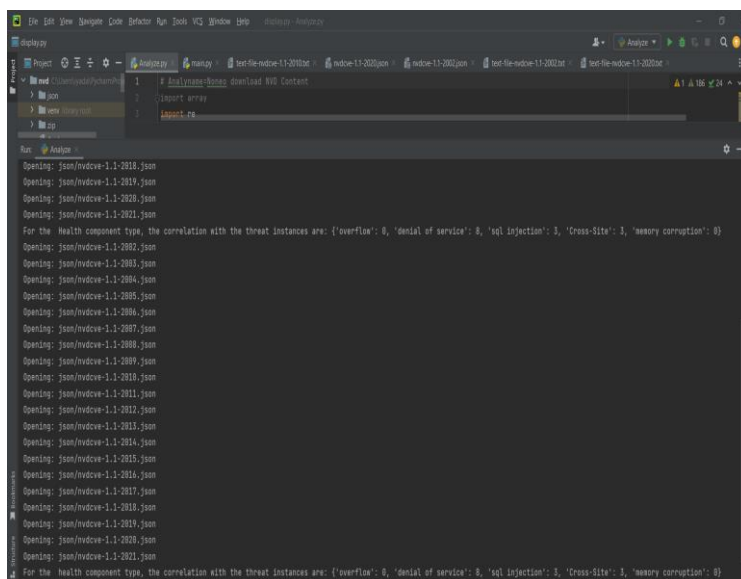


Figure. Output of tool for relating asset in the studied field (e.g. health IT asset) relate to vulnerabilities that lead to problems like denial of service, sql injection, overflow, or any other chosen by the user.

4.5 Legal interface

When the issue of disclosure and timing to report vulnerabilities is investigated, it is evident that thorough studies of other overlapping laws is needed. For instance, the MDR and NIS2 include obligations on incident notification. Article 87 MDR requires medical device manufacturers to report serious incidents to the relevant competent authorities, while Article 20(1) NIS2 requires EU Member States to oblige essential/important entities (e.g., healthcare CI) to send the notifications of significant security incidents without undue delay. Despite the different definitions in both legislations, applying both can lead to overlapping work for medical device manufacturers. In fact, the problem is in the interpretation of both obligations in the case of overlap. One aiding factor is Article 2(6) NIS2 that articulates the case when incident notification overlaps with another specific law (legislation specific to the application e.g., MDR), and it explains that the specific-sector legal-codes should prevail if “those requirements are at least equivalent in effect to the obligations laid down in this Directive” (NIS2, 2022:31). The problem in the interpretation here lies in the vague phrase “at least equivalent,” which requires extra work to correctly identify and relate specifications to, especially that NIS2 does not explain what the word ‘equivalent’ refers to in this context, and it does not give examples of such handling.

Another type of problem that relates to the divergence between the MDR and NIS2 when mapping the legal code to technical specs is when the issue of time is to be interpreted. For instance, Article 20(4)(a) NIS2 mandates notification “without undue delay and in any event within 24 hours after having become aware of the incident” (NIS2, 2020:47). On the other hand, Article 87(3) MDR mandates the notification “not later than 15 days after they become aware of the incident” (MDR, 2017:73), Article 87(4) MDR mandates that if the event is

serious then the reporting should be “*not later than 2 days after the manufacturer becomes aware of that threat*” (MDR, 2017:73), and Article 87(5) MDR mandates that in the cases of death or serious deterioration of a person’s health the “*the report shall be provided immediately after the manufacturer has established or as soon as it suspects a causal relationship between the device and the serious incident but not later than 10 days after the date on which the manufacturer becomes aware of the serious incident*” (MDR, 2017:73). In studying the above few examples, it is clear that the MDR and NIS2 are not compatible nor are they equivalent. One problem in such a situation, when transforming NIS2 to a national law in Sweden and looking at the healthcare sector as a CI, is to use interpretation approaches to come up with a legal obligation that can be put in practice without leading the organization to violations of any of the legislations.

In the last example on the time of notification, the problem of mapping of NIS2 to a specification would be to find the right number of days/hours as a maximum period before reporting to the relevant authorities without violating any other relevant legislation. Several similar conflicts of obligations are problems that this thesis will tackle. To achieve the sought results, this work needs to divide the problem caused by the overlapping of laws into several subproblems. This aids in tackling each problem at a time to converge to the final solution and propound recommendations.

In breaking down the problem into subproblems, one of the steps requires mapping the legal texts to technical specifications, which is discussed via an example below in Section 4.6.

For the sake of presenting the subproblems in case the reader is interested in knowing where the mapping occurs, the following paragraph lists the fragmentation of the problem. See point (iv) below. Otherwise, the reader may jump directly to Section 4.6.

The subproblems are: (i) reviewing the EU legislation articles specific to the main problem (e.g., timing), (ii) investigating whether IG 2.0 and other approaches could be utilized in such a work, (iii) breaking down (e.g., using IG 2.0) each selected article into attributes, deontic, aim, and object (iv) mapping the related obligations/objectives into technical controls or specs that are practically deployable in healthcare CIs in Sweden, (v) validating the resulting technical specs to ensure legal compliance with the NIS2 Directive and other relevant Swedish and EU legislations (e.g., SFS 2022:508 and MDR), (vi) communicating the resulting mapping to managers and technical personnel in a clear and concise manner, and (vii) investigating the monitoring/auditing of the implementation of the resulting table of technical controls/specs via investigating several monitoring models or tools to ensure the ongoing compliance of the healthcare organizations in Sweden that use such controls/specs with the NIS2 Directive.

4.6 Mapping to technical specifications: tables and algorithms

After locating the overlap between NIS2 with other legal instruments based on the type of industry (e.g., healthcare), the work moves to transforming the legal instructions to technical specification parameters regarding the timing of reporting and disclosure. The best way to understand this issue is via an example. This section considers the articles discussed above in Section 4.5 to show how the transformation from legal text of provisions can end in a technical specification.

This specification can be in the form of numbers, algorithms, or any other technical form.

In this respect, Article 20(4)(a) NIS2 mandates notification *“without undue delay and in any event within 24 hours after having become aware of the incident”* (NIS2, 2020:47).

At the same time, the MDR is more pedantic in its division of timing specifications when it comes to incident reporting, and it discussed three cases:

- Case 1: Article 87(3) MDR mandates the notification *“not later than 15 days after they become aware of the incident”* (MDR, 2017:73).
- Case 2: Article 87(4) MDR mandates that if the event is serious then the reporting should be *“not later than 2 days after the manufacturer becomes aware of that threat”* (MDR, 2017:73)
- Case 3: Article 87(5) MDR mandates that in the cases of death or serious deterioration of a person’s health the *“the report shall be provided immediately after the manufacturer has established or as soon as it suspects a causal relationship between the device and the serious incident but not later than 10 days after the date on which the manufacturer becomes aware of the serious incident”* (MDR, 2017:73).

The above example shows four (4) compliance statements for the same issue, that of reporting an incident. One of them is from NIS2 (directive) while the other three are from a different law (MDR). However, all the four provisions overlap and apply to InfoSec for health and medical devices reporting and timing. To solve the confusion of this overlap, referral to the dogmatic method is needed to render the interpretation using the legal interpretation techniques presented in Appendix 3) is used. Then it derives to a sort of algorithm and table of specifications.

A note worth mentioning after reading the above excerpts from NIS2 and the MDR is that the reader can notice that the MDR and NIS2 are not compatible nor are they equivalent.

Going back to the articles, in Article 20(4)(a) NIS2 *“without undue delay”* means 24 hours are counted from the point in time when the entity was aware of the occurrence of the incident.

Transforming this into a technical specification means:

- Firstly, noting down on paper or via and automation (tool) how and when the awareness about the incident happens.
- Secondly, deciding on the time limit
- Thirdly, changing the limit from the written values to computer usable number e.g., seconds.

Hence, the article requires starting to count a certain number of hours (24), which is not a unit very much used by computers. Hence, the units in provisions need to be checked. When doing so, the result would be a technical specifications table (see Table 3).

Table 3. sample technical specifications table for InfoSec parameters needed for reporting incidents while being compliant with NIS2.

Parameter	Given Unit	Computer Utilizable?	Value	Related Technical Variable	Unit	Value
Time	Hour	No	24	Type: integer	seconds	86400
				Name: ReportCounter		

Hence, the InfoSec operational and technical departments know that they need to set up a computer program with a counting variable called ReportCounter which is initialized to 86400 e.g., ReportCounter == 86400.

Hence, an important part of transforming to technical specifications is to decide on the unit of the technical spec.

Moving to the MDR articles, this section analyzes the three cases provided above based on the three MDR articles. This would result in the following summary of cases for a technical specification purpose. The MDR cases are:

- Case 1: 15 days for manufacturer, if incident is normal;
- Case 2: 2 days if incident is serious;
- Case 3: 0 days in cases of death per or if there is serious health deterioration, and 10 days for manufacturer.

Since there are cases, then this is a clear call for the technical specification to be a coded algorithm. To do so, the algorithm needs a variable to use the condition of cases on. This section chooses InciCon which stands for incident condition.

Adding the case derived from NIS2, then InciCon has 4 possible cases:

- o 1 for normal
- o 2 for serious
- o 3 for very serious.

Combining all these results in one table we get the result shown in Table 4.

Table 4. sample technical specifications table for InfoSec parameters needed for reporting incidents while being compliant with NIS2.

Legal Instrument	Cases	Parameter	Given Unit	Computer Utilizable?	Value	Related Technical Variable	Unit	Value
NIS2	1	Time	Hour	No	24	Type: integer	seconds	86 400
						Name: ReportCounter		
MDR	3	1- Time + normal	days	No	15	Type: integer	seconds	1 296 000
						Name: ReportCounter		
		2- Time + serious	days	No	2	Type: integer	seconds	172 800
						Name: ReportCounter		
		3- Time + very serious	days	No	0 (established) + 10 (aware)	Type: integer	seconds	0
						Name: ReportCounter		864 000

At this point the researcher needs to find the common denominators between NIS2 and MDR based on the cases. In doing so, this section resulted in the following specification algorithm.

```
-----  
If (InciCon = 1 OR 2) Then  
    Revert to NIS2(.);  
    ReportCounter = 86400;  
  
Else If (InciCon = 3) Then  
    Revert to MDR(.);  
    ReportCounter = 0;  
  
Else Do Wait(Input)  
  
End-If  
-----
```

This means that having NIS2 makes 2 cases the MDR converge to one case, that of NIS2. This is one result that takes a lot of the burden off the shoulders of technical InfoSec groups. This is because instead of reading 4 provisions and trying to interpret them, they just get a pseudocode algorithm like the above one or at least a 'case-based conditional-list' that shows that the technical implementation of NIS2 and MDR for timing is simpler than it looks like in the legal texts.

5. Discussion

This chapter includes the analysis and discussion of the results in relation to the previous research, impact of methods on the results, and the possible societal and ethical concerns. The Discussion also addresses whether the results may be interpreted in a different way, and if they are applicable. Since the results are shown to be applicable and a tool was created to aid in proving so, a discussion on the meaning of the results for practical activities is articulated.

The rest of this chapter is organized as follows. Section 5.1 discusses the thesis results in relation to the previously published research. Section 5.2 elaborates on the relationship of the selected methods and the achieved results. Section 5.3 deliberates the ethical and societal aspects of the study.

5.1 Previous research

This section discusses the identified results in Chapter 4 in relation to the previously published research. Potential limitations in any research work should be discussed by the researcher (Berndtsson et al. 2008). One of the issues of concern in the previous research that affects the work in this thesis and any work on InfoSec is that there is not a universally adopted definition for InfoSec. Accordingly, many definitions of InfoSec with different scopes are provided by different organizations and entities (Horne et. al, 2016). Being aware of this issue, the researcher in the field of InfoSec better be aware of the possible effects of the lack of a common definition on the usability and reliability of results.

Moreover, the main legal instrument under study (NIS2) does not provide a definition for the exact term ‘information security.’ This adds to the blend of issues to consider so that there would be no confusion about what to include in the study when InfoSec is concerned with in this multidisciplinary thesis (InfoSec and Law). Subsections 2.1.3 adopts an InfoSec definition, and Subsection 4.1 articulates the interpretation of the NIS2 para 79 to show that the right and suitable InfoSec definition is the one provided in the ISO/IEC 27000:2018 standard. It defines InfoSec as the “preservation of confidentiality, integrity and availability” (CIA) of information (ISO, 2018:3.28).

This thesis result helps simplify the interpretation for InfoSec when working with NIS2 to provide technical specifications. It is a positive result according to Paananen et. al (2020). It is advantageous to set such a bedrock for the research for similar work approach based on one definition regarding the InfoSec provisions (Paananen et. al, 2020), and it follows for linking them to technical specifications. This is because confusion can be carried to the results and lead not only to a definition discourse on InfoSec but also a problem about what technical activities must be deployed based on systematic technical specifications in InfoSec.

The results of the content analysis phase revealed that transforming NIS2 legal provisions to technical specifications is not a simple task and there is no single technique that can be used for all articles. This is shown in the result where IG 2.0 was found to be possible to apply to only a few legal articles (see Section 4.3). This result goes in harmony with the previous research especially on IG 2.0, which is still under discourse for whether it is useful for institutional rules, policies, or legal text. It is worth mentioning that this result does not mean that IG 2.0 is not suitable for interpreting laws. What the thesis conveys is that it was proven to apply to a few articles taking into consideration the healthcare CIs and

the aim of systematic establishment of technical specifications based on a provision.

Regarding the result on the socio-technical links, the previous research shows one problem area in the implementation part of legal instruments, which is shown in (Figure 9). As Kowalski (1994) shows, in most institutions, there is a problem in the chronological steps in this matter, where the administration seems to perform testing before implementation. The thesis work shows via the results on the method to transform legal provision to technical specification together with the result of the supporting computer tool (see Appendices 1 and 2) that this gap or confusion (Figure 9) is addressed. Moreover, guidance can be given to render the implementation. The tool can also aid the implementation phase since it can automate the searches for required vulnerabilities to be reported for compliance with NIS2 more quickly than doing so manually. However, these two combined results do not solve the issue of testing since rigorous testing for all cases is not done, however, the use of the tool can provide a partial test so far. Nonetheless, a full one to prove the concept is needed.

In addition, the result of looking at the overlap with other legal instruments is crucial to look at and would not have been reached without the thorough study of previous research. In this regard, conflict of laws is a subset field in legal studies that garners major attention especially in international law as apparent in the thesis also when EU legislations are to be considered (EU regulations and directives fall under international law). Hence, the previous research is pivotal in this regard (Biasin and Kamenjašević, 2022). In brief, such results are directly affected by previous research and would not be accomplished in the right way within the given time if no prior research was conducted in this field.

5.2 Methods and results

This section elaborates on the relationship of the selected methods in the thesis and the achieved results. This thesis adopts two methods. Firstly, it conforms to the qualitative approach (see Figure 5), and the source of data is documents (see Figure 6 and Figure 7). Secondly, since the main document under study is a legal instrument (NIS2), and since other legal documents are studied, the dogmatic method is referred to only when there is a need for legal analysis, interpretation, or hierarchy of laws as described above in Section 3.7. This referral is implemented via the seven (7) steps of the dogmatic framework articulated in Hutchinson and Duncan (2012). Hence, triangulation is used since the thesis conforms to blending two research methods. The implementation of the qualitative approach is done in two steps, data collection (Section 3.3), and data analysis (Section 3.4) as shown in Figure 6 and Figure 7. In this regard, there are some limitations that should be discussed.

The first limitation is that of time since an EU directive like NIS2 needs more than the thesis period to fully consider all its articles and the intricate relations between them as discussed earlier in Section 1.5.

The measure to overcome this problem is to select several NIS2 articles that are well representative to show that the work can arrive at the sought results.

The second issue to consider is the fact that adopting two research methods requires careful attention when arriving at results so that the different perspectives of the methods do not lead to contradictory results. The thesis work took measures to overcome this issue via using the dogmatic method for only three

(3) processes: (i) considerations of the effects of hierarchy of laws, (ii) legal analysis, and (iii) using legal interpretation techniques (see Appendix 3).

In what follows are several points discussing the methods and results. Firstly, the choice of the qualitative approach and the data collection scheme of 'Document studies' already set the track to follow while conducting the research. For instance, the search was always for documents related to the aims and research questions, and that led to the details of the result on overlap between NIS2 with MDR (discussed in Section 4.4).

Secondly, the choice of the dogmatic method played a role in arriving to result of using the definition of InfoSec provided in the ISO/IEC 27000:2018. This is because reaching such a result needed legal interpretations as well as legal analysis of preamble paragraphs of NIS2.

Thirdly, in the data collection and analysis phases based on the chosen research method, the work showed where and how to use IG 2.0 to link NIS2 legal provisions to InfoSec technical specifications. However, it is also important to note that this only applies to specific provisions.

Regarding the interpretation of results presented in Chapter 4, they are aligned with the research question on *'how to map selected Articles of the NIS2 EU Directive to technical specifications for the healthcare sector in Sweden.'* Hence, they could not have been interpreted in a different way. This is because the link to the socio-technical study and to technical InfoSec specifications as well as the computer program tool made to support the thesis work and help SMEs implement NIS2 and be compliant with it, all stem from the research questions and are aligned with it i.e., they are a direct outcome of the research questions.

Regarding the application of the results in general, an objective look must discuss each result on its own. The easiest result to state that it can be applied is the supporting computer program tool since it can be run on SME asset components to test for vulnerabilities that must be reported to the EU on grounds of NIS2 requirements. The same applies to the results on linking the provisions to technical specifications since the specifications are directly applicable by technical departments that are- in turn- nothing but a direct application of the NIS2 interpreted provisions. Regarding the use of IG 2.0, one cannot argue that it can be applied in general since as mentioned above, the IG 2.0 is shown in the thesis to only work for few NIS2 legal provisions that are clear and not too long. Regarding the result on the legal interface with the MDR and the AI Act, it is a result that cannot be measured for all times since the issue of having a medical device using AI is not always available. However, in such an avenue of cases, the result can be applied. Finally, regarding the result of linking to socio-technical issues, it can be applied in the case when the EU is in the pre-implementation gap shown in Figure 9 since the legal instruments and legal implementations show that.

A note worth mentioning is that there are scarce studies that tackle similar research questions, thus unfortunately, the thesis cannot compare how its results hold up in relation to comparable studies.

5.3 Ethical and societal aspects

This thesis tackles a sensitive area of intersection between three different industries namely IT (security), legal practice, and healthcare. As mentioned earlier, two disciplines are studied (InfoSec and law) with focus on application to

healthcare CIs. There are challenges that face such work. Some are societal and others are ethical. A few ethical limitations were discussed in Section 1.4.

When dealing with laws, then there is an issue that needs to be considered from the societal and ethical aspects at the same time. This is the issue related to the researcher's conduct of copying the law provisions as they are and interpreting them in good faith while keeping in mind the social differences between nations (e.g., EU Member States). In this regard, since the audience of such research is mainly an IT audience, then it is the ethical responsibility of the research to make sure that the provision is copied with integrity and with its entirety.

In addition, since laws change over time, one ethical aspect for the researcher to deal with is to carry the burden of making sure of the prior work as well as any amendments or promulgation of new laws. This will affect the data collection part especially when using the qualitative method type of 'Content Analysis.'

Since NIS2 is to be reflected in a national law by October 2024, the Swedish government has the responsibility to render this obligation. However, it is important to note that applying the work of this thesis within the Swedish context does not mean that it would apply in the same way in other EU Member States due to societal differences. Hence, different national sources and documents should be used for other States in relation to InfoSec, CI, and healthcare. To fit a study for all the EU is not possible due to different societal challenges, and this is why initially the EU requires each State to make its own laws that abides by the provisions of the NIS2 directive but, at the same time, keeps harmony with its local legal system as well as societal and ethical values.

Therefore, from an ethical viewpoint, it would not be reliable to assess the validity and reliability of the results of this thesis in different EU Member States. Similarly, the government in Sweden cannot carry a study on transforming EU directives to local laws from a different EU Member State and deploy it in Sweden since it would lead to unclear and unreliable results.

A note worth mentioning is that the choices of research methods can be applied in all societies but not when legal matters are considered unless a supranational or international law is to abide by.

Although the EU is positive about NIS2 implementations, without transforming its legal requirements to technical specifications in InfoSec there could be ethical responsibilities that are put on the shoulders of SME managers and technicians. This is not fair since those types of employees are not supposed to interpret legal text. Hence, the research community may have the ethical and technical responsibility to aid society to take this stride to move to NIS2 compliance in the right technical direction especially for the healthcare CIs. In this regard, a concern would be that NIS2 may take too long to implement in an SME. This may put forward some risks for SMEs using their resources heavily to understand NIS2 instead of doing their actual jobs. The proponents of NIS2 may argue that although it may consume time, energy, and human resources, NIS2 surely has an edge within the EU since it aids in controlling and protecting the EU from possible threats. Moreover, in the Swedish context, it will aid the private and public sectors to have one way of working with InfoSec.

6. Conclusion

This thesis tackles two research questions. The first one focuses on 'how to map selected articles of the NIS2 EU Directive to technical specifications for the healthcare sector in Sweden.' The second question looks into 'what interpretation methods are required to encompass the new information security realities.' The thesis also looks at the overlap between NIS2 and other legal instruments (EU and national ones) so that the technical specifications are reliable and valid.

The work conforms to two research methods because it is multidisciplinary in nature i.e., involving InfoSec and law while focusing on healthcare CIs. The first research method is the qualitative one, and the sub approach is qualitative 'Secondar research.' Under this umbrella the type of qualitative method is 'Content Analysis.' The data collection method is 'Document Studies.'

The second research method is the dogmatic method which is often used in legal research, and it is applied for law hierarchies, source hierarchies, and legal interpretation.

Since two methods of research are involved, the triangulation technique is used. Hence, the combination of data collection and analysis techniques is used. Triangulation aids in leveraging the validity of the research and providing support for the results' evaluation (Yin 2013). The triangulation technique aids in fulfilling the aims of research by providing consistency in results, as well as reliability that is supported by previous research (see Section 5.1).

To answer the above research questions, both research methods were thoroughly used. For instance, legal interpretation techniques are used from the dogmatic method, and comparison of documents and content analysis was used from the qualitative method, where the results show that the transformation of a NIS2 article into technical specification is doable.

A definition for InfoSec to use with the NIS2 and within the scope of this thesis is provided. The adopted definition is that of InfoSec in the ISO/IEC 27000:2018 discussing the CIA-triad. The interpretation of NIS2 and the analysis to reach this decision on InfoSec definition is articulated in Section 4.1.

IG 2.0 is tried on several NIS2 articles but due to their long structures and complicated dependencies, hence, it was not always applicable. However, it has proven to be useful on a part of Article 21(2) NIS2 as discussed in Section 4.2.

A Python tool is shown to provide good support to prove the concept and aid SMEs to be compliant with NIS2. The output samples of the program written in Python are shown in Appendices 1 and 2.

A very interesting result that opens an important door for further work is the link between the focal points of work (points 1 and 2 in Figure 8) and the socio-technical framework shown in Figure 3 and Figure 9. One should not forget that almost all entities are involved in such a socio-technical flow.

This work supports organizations to be aware of the NIS2 requirements and opens the door to use strategies to create InfoSec technical specifications out of the relevant articles based on the implementation field or industry e.g., healthcare. This can aid in current understanding of the InfoSec requirements of NIS2 as a preparation for the near future (2024) when national laws are expected to be promulgated in relation to NIS2. Hence, the thesis may aid in increasing awareness about the link of NIS2 and the InfoSec technical specifications.

A very important conclusion when interpreting NIS2 is to be aware of the field/industry where the application is performed. This is because every industry has related legislation that needs to be accounted for. Thus, the conclusion is to look for legal overlaps between different laws from different disciplines. For instance, in this thesis the industry targeted is healthcare. In this regard, when interpreting NIS2, the researcher must look at InfoSec issues related to health, medicine, and medical devices. Then, an overlap was discovered between NIS2, MDR and the AI Act. This intersection of laws may lead to conflicts of laws that could create problems when transforming NIS2 provisions to technical specifications. This is shown and discussed in more detail with an example in Section 4.6.

On the other hand, some limitations and challenges face the work such as lack of time to match the size of NIS2 and other related legal instruments. Moreover, there is scarcity in resources that tackle this field.

Ethical considerations are also discussed, most importantly of which is the integrity of the researcher when copying legal provisions and interpreting legal provisions in good faith.

Achieving the thesis aims to transform provisions to InfoSec technical specifications requires a systematic approach to InfoSec in healthcare CIs. This is challenging since assets (network connected components in healthcare CIs) are not all known due to information classification.

The thesis accomplished the task of shedding a light on the topic of challenges coming from the NIS2 obligations and it pointed out important areas of intersection of laws in relation to NIS2. Evaluation of results together with reliability and validity checks are conducted.

6.1 Open issues

Some issues remain open in this research and need further study. Such issues include *inter alia*:

- 1- Interpretation of all NIS2 preamble paragraphs and the rest of articles.
- 2- Further links with the socio-technical system to investigate.
- 3- Developing the computer code to discover more vulnerabilities and analyze them.

6.2 Future work

This study investigates a timely issue in relation to the NIS2 EU Directive that poses a hard deadline (in October 2024) on EU Member States and organizations to be ready for compliance. Hence, the related future work considers near future works for meeting the deadline in 2024 as well as further developments that may be conducted after that point in time.

The main issue that this thesis investigates relates to a current need to understand NIS2 and interpret its articles so that they can be transformed into InfoSec technical controls and specs for the healthcare sector in Sweden. Such specs can then be more easily understood by technicians and managers that need to deploy InfoSec measures to be compliant with NIS2. This current need creates a larger burden when the organization is a CI, especially if it relates to life critical work i.e., a healthcare CI. Hence, the near future works can also- in turn- be seen based on the application category and the classification of the organization as a CI or not. Therefore, several aspects play a role in projecting possible future work.

While it is important to acknowledge the limitations discussed in paras 2-5 in Section 5.2 and in Section 1.4, it is worth noting that the research work has generated valuable insights that encourage further reflection. In one sense, the investigation and results of the thesis contribute to a better understanding of various socio-technical and legal aspects.

In relation to near future viewpoints to expand on this study, a follow-up on all NIS2 articles could be conducted by researchers, professors, legal practitioners, students, and managers in the law and Informatics disciplines. Involving academics would also gauge their willingness to learn about InfoSec laws, which are vital to understand especially after students graduate and need to work in the security field and comply with those laws. One idea is to incorporate a dedicated short course to this issue and more theses can be conducted in this direction. On the other hand, practitioners and researchers can try to form workgroups that tackle all NIS2 articles and use this thesis work, ideas, and results as a basis to start from.

A similar study could be carried out by international groups interested in security and law. One idea is to form international (EU) communities and domains that encourage the participation of legal practitioners and academics in law as well as their peers in the IT discipline. Such work can enhance the understanding of NIS2 more quickly to target the hard deadline in October 2024. The countdown to that deadline started in January 2023 and speedy hard work is needed to achieve practical and useful compliance results. This can be facilitated by groups that have high potential to address multidisciplinary problems. Moreover, the formation of such groups can also be useful on the long term for future EU directives and regulations.

Another path for the near future research would be to collect case studies from NIS with lessons learned while keeping the multidisciplinary aspect in the conduct of the work. This would help focus on already seen problems in transforming NIS to technical specs and would thus save time and may change some concepts in transforming the law to InfoSec specs. The near future research needs effective implementation and a plan for increasing the probability of successful compliance.

This calls for a third near future avenue in relation to NIS2, which is a study on the different factors and technical details that contribute to the failure of technically implementing previous EU directives. This would give a better understanding of failing strategies and practices that would benefit the organization by knowing what not to try before the deadline.

A fourth short term work is to conduct surveys with organizations and industry personnel to investigate what their pains are in relation to NIS2 and how they locate some of the NIS2 implementation problems. This would aid in speeding up two issues: the location of practical problems, and the creation of relevant solutions.

A fifth short term research can be inspired from the open issues (discussed above), where more tests can be rendered on the current results and the supporting tool (computer program). The tool can be enhanced to contribute more to the implementation phase (or pre-implementation gap) as shown in Figure 9.

A sixth short term work is to program the part of the tool that processes the automatic reporting based on the timing algorithm discussed in Section 4.6.

On the long term, further research could explore the simplification of NIS2 articles to create useful guidelines for managers and technicians.

Another long term work would be to create academic and industrial courses on understanding the technical implications of NIS2 and other relevant EU legislation.

A third long term research idea would be to create training workshops that focus on major implementations and that would teach both legal and IT related issues. Thus, IT experts can gain from the new legal knowledge, and legal practitioners can gain IT knowledge. This would create soft values on both sides that empower workgroups to give better results when implementing such EU directives in InfoSec.

A fourth long term study would be to investigate in more depth the overlap between NIS2 and other EU legal instruments in every discipline. For instance, thorough studies are needed to look at intersections of NIS2 with other EU legislation in the fields of energy, smart grids, nuclear power plants, water networks, aviation, healthcare, pharmaceutical companies, and more.

A fifth long term work is to develop the correlation part of the code to include issues related to the MDR.

Finally, the thesis opens two general avenues for future work in research. The first relates to investigating the use of IG 2.0 for legal statements. The second relates to the transformation of laws into technical specs via tables and algorithms. Both avenues require multidisciplinary research work as well as the co-operation between researchers and practitioners from the fields of Informatics and law.

References

- Åhlfeldt, R-M., Spagnoletti, P., and Sindre G. (2007) 'Improving the Information Security Model by using TFI', In Proceedings of the 22nd IFIP TC-11 International Information Security Conference (SEC 2007), Sandton, South Africa, 14-16 May 2007. ISBN: 13:978-0-387-72366-2, eISBN: 13:9780-387-72367-9, ISSN: 1571-5736. pp. 73-84.
- AI Act (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final (AI Act proposal).
- AlertMedia (2023). The All-Hazards Approach to Emergency Planning Explained. Emergency Management. Available at: <https://www.williamsburgva.gov/232/Emergency-Management>, last accessed 13 August 2023.
- Bell, J. (2016). *Introduktion till forskningsmetodik*. 5th edn., Lund: Studentlitteratur.
- Berndtsson, M., Hansson, J., Olsson, B. and Lundell, B. (2008). *A Guide for Students in Computer Science and Information Systems. Thesis Projects*. Springer London. Available at: <http://dx.doi.org/10.1007/978-1-84800-009-4>, last accessed 12 August 2023.
- Bernitz, U. and Kjellgren, A. (2022). *Europarättens grunder. Sjunde upplagan. Författarna och Norstedts Juridik*. ISBN 978-91-39-02480-4.
- Bernitz, U., Carlsson, M., Heuman, L., Leijonhufvud, M., Sjöberg, C. M., Seipel, P., Contradson, W. W., and Vogel, H-H (2020). *Finna Rätt: Juristens Källmaterial och arbetsmetoder. Författarna och Norstedts Juridik*. ISBN 978-91-39-20936-2.
- Bhandari, P. (2023). *What Is Qualitative Research? Methods & Examples*. Scribbr. Published on in June 2020 by. Revised in June 2023. Available at: <https://www.scribbr.com/methodology/qualitative-research/>, last accessed 12 August 2023.
- Biasin, E., and Kamenjašević, E. (2022). Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review* 2022, Vol. 3, 163–180. Available at: <https://doi.org/10.1365/s43439-022-00054-x>, last accessed 20 December 2022.
- Cambridge (2022). "Law." *Dictionary. Meaning of Law*. Available at: <https://dictionary.cambridge.org/dictionary/english/law>, last accessed 20 December 2022.
- Carlson, L. (2013). *The Fundamentals of Swedish Law*. Studentlitteratur, Lund. ISBN 978-91-44-07872-4.
- Cerulus, L. (2020). Hackers use fake WHO emails to exploit coronavirus fears. Available at: https://www.politico.eu/article/hackers-use-fake-who-emails-to-exploit-coronavirus-fears-for-gain/?fbclid=IwAR379JroScZEggppneFxE-QqMpYfKP9MoRg9ok1B-xziGkIH_3Byy1NtKjE, last accessed 10 January 2023.
- Choucri, N. (2023). *Decoding EU-GDPR*. Political Science Department. Massachusetts Institute of Technology (MIT). Available at: <https://cpsvo.org/node/92718>, last accessed 20 January 2023.

- Cornell Law School, (2022). "Legislation." Legal Information Institute. Available at: <https://www.law.cornell.edu/wex/legislation>, last accessed 20 December 2022.
- Craigien, D., Diakun-Thibault, N., and Purse, R. (2014) 'Defining Cybersecurity', Technology Innovation Management Review, Vol. of 2014(October), pp. 13-21. ISSN: 1927-0321. Available at: <https://timreview.ca/article/835>, last accessed 10 August 2023.
- Cranenburgh, A. and Garcia-Alfaro, J. (2019). An evaluation of Nessus vulnerability scanner. *Journal of Cybersecurity Education, Research and Practice*, 2019(1), 30-44.
- Creswell, J. W., and Poth, C. N. (2016). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Sage Publications.
- Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A. and Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, 11(1), p. 100. Available at: <https://doi.org/10.1186/1471-2288-11-100>.
- De Ville, J. (2010). Madness and the law: The Derrida/Foucault debate revisited. *Journal of Law and Critique*, Vol. 21, 17-37.
- Death, D. (2017) *Information Security Handbook*: Packt Publishing.
- Diamantopoulou, V., Tsohou, A., and Karyda, M. (2019). 'General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organizations' Compliance', In *Proceedings of the 16th International Conference, TrustBus 2019, Linz, Austria. 26–29 August 2019*. LNCS, 11711. pp. 94-109.
- EC (2015). Monitoring implementation of EU directives - Applying EU Law – Law Making Process- Law. Available at: https://commission.europa.eu/law/law-making-process/applying-eu-law/monitoring-implementation-eu-directives_en, last accessed 20 January 2022.
- EC (2016). Communication from the Commission - EU law: Better results through better application. Available at: https://commission.europa.eu/publications/communication-commission-eu-law-better-results-through-better-application_en, last accessed 20 January 2022.
- EC (2019). Infringement procedure - Applying EU Law – Law Making Process- Law. Available at: https://commission.europa.eu/law/law-making-process/applying-eu-law/infringement-procedure_en, last accessed 20 January 2023.
- EC (2022a). Applying EU law – Law Making Process- Law. Available at: https://commission.europa.eu/law/law-making-process/applying-eu-law_en, last accessed 20 January 2023.
- EC (2022b). Communication from the Commission – Enforcing EU law for a Europe that delivers- Communication from the Commission- Publications. Available at: https://commission.europa.eu/publications/communication-commission-enforcing-eu-law-europe-delivers_en, last accessed 20 January 2023.
- EC (2023). Case law relating to Directive (EU) 2015/1535. Internal Market, Industry, Entrepreneurship and SMEs Single Market and Standards Tools and Databases – TRIS. Available at: <https://ec.europa.eu/growth/tools-databases/tris/en/about-the-20151535/case-law/>, last accessed 20 January 2023.

- ECA (2019). Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper). European Court of Auditors (ECA). Available at: <https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=49416>, last accessed 20 January 2023.
- ECA (2022). Special report 05/2022: Cybersecurity of EU institutions, bodies and agencies : Level of preparedness overall not commensurate with the threats. European Court of Auditors (ECA). Available at <https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=60922>, last accessed 20 January 2023.
- ECA (2023). Our values, mission and vision – About us. European Court of Auditors (ECA). Available at: <https://www.eca.europa.eu/en/Pages/values-mission-and-vision.aspx>, last accessed 20 January 2023.
- ENISA (2023). Supporting the implementation of Union policy and law regarding cybersecurity- NIS Directive- Cybersecurity Policy. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new>, last accessed 20 January 2023.
- EU (2015). Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)- Legislative Acts. 17.9.2015. (I. 241/1). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535>. Last accessed 20 January 2023.
- EU (2022). “Type of Legislation.” Law - Institutions, Law, Budget. European Union. Available at: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en, last accessed 20 December 2022.
- EU (2023). “Founding agreements.” Principles and values- Principles, countries, history. Available at: https://european-union.europa.eu/principles-countries-history/principles-and-values/founding-agreements_en#:~:text=The%20European%20Union%20is%20based,a%20law%20in%20that%20area., last accessed 20 January 2023.
- Fernandi, J. (2023). Gross Domestic Product (GDP): Formula and How to Use It. Economy- Economics. Investopedia. Available at <https://www.investopedia.com/terms/g/gdp.asp>, last accessed 21 August 2023.
- Foucault, M. (1975). Discipline and Punish: The Birth of the Prison. Vintage Books. A Division of Random House, Inc. New York.
- Frantz, C. K., and Siddiki, S. (2021). Institutional Grammar 2.0: A specification for encoding and analyzing institutional design. *Journal of Public Administration*, Vol. 100, Issue 4, December 2020). John Wiley & Sons Ltd. Wiley Online Library.
- Frantz, C. K., and Siddiki, S. (2022). *Institutional Grammar*. Palgrave Macmillan. 1007/978-3-030-86372-2.
- GDPR (2018). General Data Protection Regulation. Regulation (EU) 2016/679 of The European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: <https://eur-lex.europa.eu/legal->

- content/EN/TXT/PDF/?uri=CELEX:32016R0679, last accessed 6 December 2022.
- George, T. (2023). What is Secondary Research? Definition, Types, & Examples. Qualitative vs Quantitative. Scribbr. Available at: <https://www.scribbr.com/methodology/secondary-research/>, last accessed 13 August 2023.
- Gözler, K. (2016). "The Question of the Rank of International Treaties in National Hierarchy of Norms: A Theoretical and Comparative Study", *Essays in Honor of Prof. Dr. Mehmet Genç*, (eds.) Reçber, K., Özdal, B., Özgenç, Z., and Dora, B., 21-46. Available at: <http://www.anayasa.gen.tr/rank-of-treaties.pdf>, last accessed 21 January 2023.
- Hildebrandt, M. (2020). "International and Supranational Law" in *Law for Computer Scientists and Other Folk*. Oxford University Press (OUP). ISBN: 9780198860877.
- Horne, C., Ahmad, A., and Maynard, S. (2016). *A Theory on Information Security*. In *The 27th Australasian Conference on Information Systems*. Wollongong, Australia.
- Hutchinson, T. and Duncan, N. (2012). Defining and describing what we do: doctrinal legal research. *Deakin Law Review*. Vol. 17, No. 1, pp. 83, 99.
- IG (2022). *Institutional Grammar 2.0 Quick Reference*. Uploads 2022- Institutional Grammar. Available at: <https://institutionalgrammar.org/wp-content/uploads/2022/10/Institutional-Grammar-2.0-Quick-Reference-Guide.pdf>, last accessed 20 December 2022.
- ISO (2012). *Information technology- Security techniques- Guidelines for cybersecurity* (ISO/IEC 27032:2012).
- ISO (2013). *Information technology - Security techniques – Information security management systems - requirements*. Tech. rep. (ISO/IEC 27001:2013).
- ISO (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. (ISO/IEC 27000:2018).
- ISO (2019). *Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines* (ISO/IEC 27701:2019).
- ISO (2022a). *Information technology- Security techniques- Code of practice for information security controls* (ISO/IEC 27002:2022).
- ISO (2022b). *Information technology- Security techniques- Information security management systems- Overview and vocabulary*, 5th ed (ISO/IEC 27001:2022). Available at: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:vi:en>, last accessed 10 August 2023.
- Jesson, J., & Lacey, F. (2006). How to do (or not to do) a critical literature review. *Pharmacy Education*, 6(2), 139–148. Available at <https://doi.org/10.1080/15602210600616218>, last accessed 12 August 2023.
- JHLL (2019). *Legal Dissertation: Research and Writing Guide*. Research Guides. Jerome Hall Law Library. Maurer School of Law. Available at: <https://law.indiana.libguides.com/dissertationguide#s-lg-box-22069151>, last accessed 21 August 2023.

- JHLL (2019). Legal Dissertation: Research and Writing Guide. Research Guides. Jerome Hall Law Library. Maurer School of Law. Available at: <https://law.indiana.libguides.com/dissertationguide#s-lg-box-22069151>, last accessed 21 August 2023.
- Kebede, A. (2002). John Rawls and Jean-François Lyotard on Pluralism: Themes of Convergence and Divergence. *Journal of Social Thought & Research*, Vol. 25, No. 1/2, Postmodernism, Globalization, and Politics 2002, pp. 111-141.
- Kianpour, M. and Frantz, C. (2021) Analysis of institutional design of EU cyber incidents and crises management as a complex public good. Under review in *Policy Studies Journal*.
- Kilcommins, S. (2016). Doctrinal Legal Method (Black-Letterism): Assumptions, Commitments and Shortcomings. In Cahillane, L. and Schweppe, J. (eds) *Legal Research Methods: Principles and Practicalities*. Clarus Press Ltd. Dublin.
- Kilcommins, S. (2016). Doctrinal Legal Method (Black-Letterism: Assumptions, Commitments and Shortcomings. In Cahillane, L. and Schweppe, J. (eds) *Legal Research Methods: Principles and Practicalities*. Clarus Press Ltd. Dublin.
- Knapp, E., D. and Langill, J., T. (2015). *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. 2nd edn. Syngress, Elsevier. ISBN: 978-0-12-420114-9.
- Kowalski, S. (1994). *IT Insecurity: A Multi-disciplinary Inquiry*. Doctoral Thesis. The Department of Computer and Systems Sciences (DSV) at Stockholm University (SU) and The Royal Institute of Technology (KTH). Report Series No. 94-004. ISSN 1101-8526. ISRN SU-KTH/DSVR-94/4--SE. ISBN: 91-7153-207-2.
- Lancet, T. (2023). Facts about ScienceDirect. Available at: <https://www.elsevier.com/solutions/sciencedirect>, last accessed 12 August 2023.
- Lekshmi, S. A. (2022). Growing concern on healthcare cyberattacks & need for cybersecurity. PsyArXiv. Available at: <https://doi.org/10.31234/osf.io/7m4qf>, last accessed 10 January 2023.
- Lyon, D. (2017). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. O'Reilly Media, Inc.
- Lyotard, J-F., Hudek, A., and Lydon M. (2020). Discourse. University of Minnesota Press Stable. 327-355. Available at: https://www.jstor.org/stable/10.5749/j.ctttfd2.17#metadata_info_tab_contents, last accessed 6 December 2020.
- Macrotrends (2023). Sweden Healthcare Spending 2000-2023. Available at: <https://www.macrotrends.net/countries/SWE/sweden/healthcare-spending>, last accessed 20 January 2023.
- Maglaras, L., Drivas, G., Noou, K., and Rallis, S. (2018). NIS directive: The case of Greece. *EAI Endorsed Transactions on Security and Safety*, Vol. 4, No. 14 (2018).
- Markopoulou, D., Vagelis Papakonstantinou, V., and de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law & Security Review*, Vol. 35, Issue 6, November 2019, 105336.
- McClintock, T. (2020). Without Law Enforcement There is No Law, and Without Law There is No Civilization. *Thoughts on Police Reform*. California Globe.

- Articles. Available at: <https://californiaglobe.com/articles/without-law-enforcement-there-is-no-law-and-without-law-there-is-no-civilization/>, last accessed 6 December 2022.
- McCrudden, C. (2006). Legal Research and the Social Sciences. *Law Quarterly Review* 2006. 632-650.
- MDR (2017). Medical Device Regulation. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. *Official Journal of the European Union* L 117/1. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745>, last accessed 20 January 2023.
- Merriam-Webster (2022). "Regulation." Dictionary. Available at: <https://www.merriam-webster.com/dictionary/regulation>, last accessed 20 December 2022.
- Ministry of Justice (2016). The Swedish Law-Making Process. Fact Sheet. Ju16.03e. Government Offices of Sweden. Available at: <https://www.government.se/49c837/contentassets/4490fe7afcbo40b0822840fa460dd858/the-swedish-law-making-process>, last accessed 20 December 2022.
- Mitre (2023). CVE database. CVE Program. Available at: https://cve.mitre.org/cve/search_cve_list.html, last accessed 21 August 2023.
- MSB (2014). Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure. Swedish Civil Contingencies Agency (MSB). Risk & Vulnerability Reduction Department. Natural Hazards & Critical Infrastructure Section. ISBN: 978-91-7383-447-6. Available at: <https://www.msb.se/siteassets/dokument/publikationer/english-publications/action-plan-for-the-protection-of-vital-societal-functions--critical-infrastructure.pdf>, last accessed 20 January 2023.
- NIS (2018). Network and Information Systems (NIS) Directive. EU 2016/1148. European Union Agency for Cybersecurity (ENISA). Available at: <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new>, last accessed 6 December 2022.
- NIS2 (2020). Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. COM (2020) 823 final. 2020/0359 (COD). European Union Agency for Cybersecurity (ENISA). Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF, last accessed 6 December 2022.
- NIS2 (2022). The NIS 2 Directive. Available at: <https://www.nis-2-directive.com/>, last accessed 20 December 2022.
- NIST (2013). Glossary of Key Information Security Terms. Revision 2. NIST IR 7298 r2. (National Institute of Standards and Technology. US Department of Commerce. Available at: <https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>
- Okoli, C., (2015). "A Guide to Conducting a Standalone Systematic Literature Review." *Communications of the Association for Information Systems*. Vol. 37.

- Article 43. Available at: <https://aisel.aisnet.org/cais/vol37/iss1/43>, last accessed on 20 January 2023.
- Okoli, C., and Schabram, K. (2010). Working Papers on Information Systems A Guide to Conducting a Systematic Literature Review of Information Systems Research. Working Papers on Information Systems, 10(2010). <https://doi.org/10.2139/ssrn.1954824>.
- Otto, P. N., and Antón, A. I. (2007) Addressing Legal Requirements in Requirements Engineering. The 15th IEEE International Requirements Engineering Conference, India Habitat Centre, New Delhi (15-19 October 2007) . Available at IEEE Computer Society: 10.1109/RE.2007.65.
- Paananen, H., Lapke, M. and Siponen, M. (2020). State of the art in information security policy development. Computers & Security, 88, p. 101608. Available at: <https://doi.org/10.1016/j.cose.2019.101608>, last accessed 12 August 2023.
- Pasquale, F. (2019), A Rule of Persons, Not Machines: The Limits of Legal Automation. The George Washington Law Review (January 2019) Vol. 87, No. 1.
- Patel, R. and Davidson, B. (2019). Forskningsmetodikens grunder. 5th ed., Lund: Studentlitteratur.
- Regeringskansliet (2021). Svara på remiss – om remisser av betänkanden och andra förslag från Regeringskansliet. Available at: <https://www.regeringen.se/rapporter/2021/09/svara-pa-remiss/>, last accessed 20 January 2023.
- Regeringskansliet (2022). Remisser. Remiss från Justitiedepartementet. (Publicerad 21 juni 2022). Available at: <https://www.regeringen.se/remisser/2022/06/inkomstskatterapporter-och-nagra-redovisningsfragor-sou-202229/>, last accessed 20 January 2023.
- Riksdagen (2021a). What does the Riksdag do? Sveriges Riksdag. Available at: <https://www.riksdagen.se/en/how-the-riksdag-works/what-does-the-riksdag-do/>, last accessed 20 January 2023.
- Riksdagen (2021b). Works with EU matters. Sveriges Riksdag. Available at: <https://www.riksdagen.se/en/how-the-riksdag-works/what-does-the-riksdag-do/works-with-eu-matters/>, last accessed 20 January 2023.
- Riksdagen (2022a). Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster t.o.m. SFS 2022:508. Dokument & lagar. Sveriges Riksdag. Available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174, last accessed 20 January 2023.
- Riksdagen (2022b). Beslutar om lagar. Available at: <https://www.riksdagen.se/sv/sa-funkar-riksdagen/riksdagens-uppgifter/beslutar-om-lagar/#:~:text=del%20av%20svaren,-,F%C3%B6rslag%20fr%C3%A5n%20regeringen,d%C3%A5%20utredningen%20av%20p%C3%A5%20remiss>, last accessed 20 January 2023.
- Romanosky, S., Ablon, L., Kuehn, A., and Jones, T. (2019). Content analysis of cyber insurance policies: how do carriers price cyber risk?, Journal of Cybersecurity, Vol. 5, Issue 1., <https://doi.org/10.1093/cybsec/tyz002>, last accessed 13 August 2023.
- Saunders, M., Lewis, P. and Thornhill, A. (2007). Research Methods for Business Students. 4th ed., Harlow: Pearson Education Limited.

- SCB (2023). National Accounts, quarterly and annual estimates. Official statistics of Sweden. Statistikmyndigheten. Available at: <https://www.scb.se/en/finding-statistics/statistics-by-subject-area/national-accounts/national-accounts/national-accounts-quarterly-and-annual-estimates/>, last accessed 21 July 2023.
- Schwartz, M. (2020). COVID-19 complication: ransomware keeps hitting healthcare. Available at: <https://www.bankinfosecurity.com/covid-19-complication-ransomware-keeps-hitting-hospitals-a-13941>, last accessed 10 January 2023.
- SFS (2018a). Lag om informationssäkerhet för samhällsviktiga och digitala tjänster. (SFS 2018:1174). Försvarsdepartementet.
- SFS (2018b). Säkerhetsskyddslag (2018:585). Available at https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585/#K1, last accessed 10 August 2023.
- SFS (2018c). Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. (SFS 2018:1175).
- SFS (2018d). *Säkerhetsskyddsförordning* (2018:658). Available at: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddsforordning-2018658_sfs-2018-658/#K1, last accessed 10 August 2023.
- Sharma, P. and Nagpal, N. (2017). A comparative analysis of vulnerability assessment tools: Metasploit, Nessus, and Nexpose. In 2017 IEEE 7th International Conference on Advances in Computing, Communications, and Informatics (ICACCI), 2501-2505.
- SI (2021). "Swedish healthcare is largely tax-funded. And the overall quality is high." Healthcare in Sweden. Swedish Institute- Sweden. Available at: <https://sweden.se/life/society/healthcare-in-sweden>, last accessed 20 December 2022.
- Smedinghoff, T. J. (2008). Information Security Law: The Emerging Standard for Corporate Compliance. IT Governance Publishing. ISBN:978-1-905356-67-6. Available at: <https://www.jstor.org/stable/j.ctt5hh7kw>, last accessed 6 December 2022.
- Smits, J. M. (2017). What Is Legal Doctrine? In van Gestel, R., Micklitz, H-W., Rubin, E. L. (eds). Rethinking Legal Scholarship: A Transatlantic Dialogue, pp. 207-228. Cambridge University Press. ISBN:9781316442906.
- Statista (2022). Public expenditure in Sweden in 2021, by function. Economy & Politics-Politics & Government. Statista Research Department. Available at: <https://www.statista.com/statistics/530145/swedenpublic-expenditure-by-function/>, last accessed 20 December 2022.
- Streubert, H. J., and Carpenter, D. R. (1999). Qualitative Research in Nursing: Advancing the Humanistic Imperative. 2nd ed. Philadelphia: J.B. Lippincott.
- Susanto, A., Lee, H., and Zo, H (2011). Factors Influencing Initial Trust Formation in Adopting Internet Banking in Indonesia. Conference: The IEEE International Conference on Advanced Computer Science and Information System (December 2011). ICACSI 2011 ISBN: 978-979-1421-11-9.

- Tessian (2021). '20 Biggest GDPR Fines of 2019, 2020, and 2021 (So Far)', DLP Compliance. Available at: <https://www.tessian.com/blog/biggest-gdpr-fines-2020/>, last accessed 6 December 2022.
- The White House (2022). The Legislative Branch. Available at: <https://www.whitehouse.gov/about-the-white-house/our-government/the-legislative-branch/>, last accessed 20 December 2022.
- Thombre, S. (2019). "General principles of statutory interpretation with special reference to golden rule & mischief rule" *International Journal of Law*, ISSN: 2455-2194, Vol 5, Issue 6 (November 2019) 135-140.
- Tyani, E. E. (2023). A Vulnerability Assessment Approach for Home Networks (A case of Cameroon). Master Thesis. Department of Informatics. University of Skövde (HIS).
- Vidich, S. (2023). ISO/IEC 27701:2019. Learn — Azure Compliance — Azure Compliance Offerings — Global. Microsoft. Available at: <https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-iso-27701>, last accessed 21 August 2023.
- von Solms, R., and van Niekerk, J. (2013), From information security to cyber security. *Computer and Security*, 38, Elsevier, pp. 97-102. Available at: <https://linkinghub.elsevier.com/retrieve/pii/S0167404813000801>, last accessed 10 August 2023.
- Wolford, B. (2023). What is GDPR, the EU's new data protection law? GDPR.EU Project. Available at: <https://gdpr.eu/what-is-gdpr/>, last accessed 21 August 2023.
- Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, 19(3), pp. 321–332. Available at: <https://doi.org/10.1177/1356389013497081>.
- Zalnieriute, M., Moses, L. B., and Williams, G. (2019). The Rule of Law and Automation of Government Decision-Making. *Modern Law Review* 82(3) UN-SWLRS 14.

Appendices

Appendix 1

Vulnerability Detection and Reporting Tool: Sample Primary Output

Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L)."

Example:

```
{
  "cve" : {
    "data_type" : "CVE",
    "data_format" : "MITRE",
    "data_version" : "4.0",
    "CVE_data_meta" : {
      "ID" : "CVE-2023-21923",
      "ASSIGNER" : "secalert_us@oracle.com"
    },
    "problemtype" : {
      "problemtype_data" : [ {
        "description" : [ {
          "lang" : "en",
          "value" : "NVD-CWE-noinfo"
        } ]
      } ]
    },
    "references" : {
      "reference_data" : [ {
        "url" : "https://www.oracle.com/security-alerts/cpuapr2023.html",
        "name" : "https://www.oracle.com/security-alerts/cpuapr2023.html",
        "refsource" : "MISC",
        "tags" : [ "Patch", "Vendor Advisory" ]
      } ]
    },
    "description" : {
      "description_data" : [ {
        "lang" : "en",
        "value" : Vulnerability in the Oracle Health Sciences InForm product of Oracle Health Sciences Applications (component: Core). Supported versions that are affected are Prior to 6.3.1.3 and Prior to 7.0.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences InForm. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Health Sciences InForm accessible data as well as unauthorized access to critical data or complete access to all Oracle Health Sciences InForm accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Health Sciences InForm. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L)."
      } ]
    },
    "configurations" : {
      "CVE_data_version" : "4.0",
      "nodes" : [ {
        "operator" : "OR",
        "children" : [ ],
        "cpe_match" : [ {
          "vulnerable" : true,
          "cpe23Uri" : "cpe:2.3:a:oracle:health_sciences_inform:7.0.0.0:*:*:*:*:*:*",
          "cpe_name" : [ ]
        }, {
          "vulnerable" : true,
          "cpe23Uri" : "cpe:2.3:a:oracle:health_sciences_inform:*:*:*:*:*:*",
          "versionEndExcluding" : "6.3.1.3",
          "cpe_name" : [ ]
        } ]
      } ]
    },
    "impact" : {
      "baseMetricV3" : {
```

```

"cvssV3" : {
  "version" : "3.1",
  "vectorString" : "CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L",
  "attackVector" : "NETWORK",
  "attackComplexity" : "LOW",
  "privilegesRequired" : "LOW",
  "userInteraction" : "NONE",
  "scope" : "UNCHANGED",
  "confidentialityImpact" : "HIGH",
  "integrityImpact" : "HIGH",
  "availabilityImpact" : "LOW",
  "baseScore" : 8.3,
  "baseSeverity" : "HIGH"
},
"exploitabilityScore" : 2.8,
"impactScore" : 5.5
}
},
"publishedDate" : "2023-04-18T20:15Z",
"lastModifiedDate" : "2023-04-20T13:18Z"
},

```

Appendix 2

Output of Python Tool for Compliance with Article 21 NIS2

Code Correlating Healthcare Vulnerabilities with other IT specs

Part of the tool for compliance with the selected NIS2 Articles of this thesis and based on the above results (presented in Chapter 5) works on locating the vulnerabilities as per the NIS2 requirement (mainly Articles 11 and 12 NIS2). Then the tool allows the user (e.g., SME) to also enter the parameters that are of interest to check the healthcare in component (asset) in the CI against i.e., whether this asset under investigation (based on NIS2 compliance) correlates with other security outcome errors (entered as program parameters) that are of interest.

An example of a set such parameters (reflecting vulnerabilities that can be correlated with the asset in the Healthcare CI) is as follows:

Correlation of Health/health with multiple security outcome errors:

- **Overflow:** an error that occurs when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage. This vulnerability can cause a system crash or, worse, create an entry point for a cyberattack.
- **DoS (Denial of Service):** describes the goal of a class of cyber-attacks designed to render a service inaccessible. The DoS attacks that most people have heard about are those launched against high profile websites, since these are frequently reported by the media.
- **XSS (Cross-Site Scripting):** attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.
- **SQL injection:** is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques
- **Memory corruption:** can be described as the vulnerability that may occur in a computer system when its memory is altered without an explicit assignment. The contents of a memory location are modified due to programming errors which enable attackers to execute an arbitrary code.

The program was made with Python and run on the following specs:

- Processor: Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz 1.19 GHz
- Installed RAM:: 8,00 GB (7,79 GB usable)
- System type: 64-bit operating system, x64-based processor
- Edition: Windows 10 Home
- Version: 22H2
- OS build : 19045.2846
- Experience: Windows Feature Experience Pack 120.2212.4190.0

The time that the Python tool to render the correlation results for the asset was: 55 seconds.

Program output sample in relation to the above example of set of parameters (security related technical errors):

```
-----
C:\Users\iyada\PycharmProjects\nvd\venv\Scripts\python.exe C:/Users/iyada/PycharmPro-
jects/nvd/Analyze.py
Opening: json/nvdcve-1.1-2002.json
Opening: json/nvdcve-1.1-2003.json
Opening: json/nvdcve-1.1-2004.json
Opening: json/nvdcve-1.1-2005.json
Opening: json/nvdcve-1.1-2006.json
Opening: json/nvdcve-1.1-2007.json
Opening: json/nvdcve-1.1-2008.json
Opening: json/nvdcve-1.1-2009.json
Opening: json/nvdcve-1.1-2010.json
Opening: json/nvdcve-1.1-2011.json
Opening: json/nvdcve-1.1-2012.json
Opening: json/nvdcve-1.1-2013.json
Opening: json/nvdcve-1.1-2014.json
Opening: json/nvdcve-1.1-2015.json
Opening: json/nvdcve-1.1-2016.json
Opening: json/nvdcve-1.1-2017.json
Opening: json/nvdcve-1.1-2018.json
Opening: json/nvdcve-1.1-2019.json
Opening: json/nvdcve-1.1-2020.json
```

```
Opening: json/nvdcve-1.1-2021.json
For the Health component type, the correlation with the threat instances are: {'overflow':
0, 'denial of service': 8, 'sql injection': 3, 'Cross-Site': 3, 'memory corruption': 0}
Opening: json/nvdcve-1.1-2002.json
Opening: json/nvdcve-1.1-2003.json
Opening: json/nvdcve-1.1-2004.json
Opening: json/nvdcve-1.1-2005.json
Opening: json/nvdcve-1.1-2006.json
Opening: json/nvdcve-1.1-2007.json
Opening: json/nvdcve-1.1-2008.json
Opening: json/nvdcve-1.1-2009.json
Opening: json/nvdcve-1.1-2010.json
Opening: json/nvdcve-1.1-2011.json
Opening: json/nvdcve-1.1-2012.json
Opening: json/nvdcve-1.1-2013.json
Opening: json/nvdcve-1.1-2014.json
Opening: json/nvdcve-1.1-2015.json
Opening: json/nvdcve-1.1-2016.json
Opening: json/nvdcve-1.1-2017.json
Opening: json/nvdcve-1.1-2018.json
Opening: json/nvdcve-1.1-2019.json
Opening: json/nvdcve-1.1-2020.json
Opening: json/nvdcve-1.1-2021.json
For the health component type, the correlation with the threat instances are: {'overflow':
0, 'denial of service': 8, 'sql injection': 3, 'Cross-Site': 3, 'memory corruption': 0}

Process finished with exit code 0
-----
```

Appendix 3

Legal Interpretation methods and techniques

Legal Interpretation methods (Bernitz, 2020):

- Linguistic interpretation. cf. the principle of legality, legal certainty
- Systematic interpretation. rule systematics and harmony, cf. main rule and exceptions
- Purpose interpretation. What was the intention of the provision? Cf. preparatory works, EU preambles
- End Goal interpretation, effects and functions of the provision, cf. argument of consequence, cf. further simplicity, efficiency

Legal Interpretation techniques (Bernitz, 2020):

- Convention, treaty or directive-compliant interpretation
- Extensive or restrictive interpretation
- Analogies (cf. induction and reduction)
- Opposite interpretation (e contrario) (should be careful with)

Appendix 4

Article 21 NIS2

Article 21

Cybersecurity risk-management measures

1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- (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.

3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure

development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

EN Official Journal of the European Union 27.12.2022 L 333/127

5. By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

The Commission may adopt implementing acts laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, of the measures referred to in paragraph 2 with regard to essential and important entities other than those referred to in the first subparagraph of this paragraph.

When preparing the implementing acts referred to in the first and second subparagraphs of this paragraph, the Commission shall, to the extent possible, follow European and international standards, as well as relevant technical specifications. The Commission shall exchange advice and cooperate with the Cooperation Group and ENISA on the draft implementing acts in accordance with Article 14(4), point (e).

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).
