UiO : Faculty of Law
University of Oslo

Manage risks to achieve an appropriate level of security

To what extent does security requirements imposed on critical sectors align with a high common level of security on network and information systems?

Candidate number: 9027

Submission deadline: 30.01.2020

Number of words: 17428

Table of contents

LIST OF ABBREVIATIONS 1

1 INTRODUCTION 2

1.1 Research question 4

1.2 Methodology 5

1.3 Structure 7

1.4 Demarcations 8

2 BRIEF ON NIS DIRECTIVE SECURITY REQUIREMENTS 9

2.1 Policy rationale 9

2.2 Background and purpose 10

2.3 The EU regulatory landscape of cybersecurity requirements 12

3 ACTORS SUBJECT TO THE DIRECTIVE 13

3.1 Operators of essential services (OES) 13

3.1.1 Consistency differences 16

3.1.2 Considerations and discussion 20

3.2 Digital service providers (DSP) 21

4 THE CONTENT OF SECURITY REQUIREMENTS 23

4.1 Security requirements are part of culture of risk management 23

4.2 Security requirements imposed on OES 24

4.3 Security requirements imposed on DSP 26

4.4 Comparing NISD and GDPR security requirements 29

5 THE IMPLEMENTATION OF SECURITY REQUIREMENTS 32

5.1 What is “appropriate and proportionate?” 32

5.1.1 Risk management 33

5.1.2 Preventative measures 34

5.1.3 The importance of certification 34

5.1.4 The role of voluntary standards 35

5.1.5 The role of “state of the art”? 36

5.1.6 Considerations 37

5.2 Comparing the implementation of security requirements in Member States 38

5.2.1 Three dimensions of implementation in EU countries 38

5.3 The case of Norway: comparing NISD with Sikkerhetsloven 40

5.4 Achieving a “high common level”? 41

5.5 Judicial policy considerations 42

6 CONCLUSION 44

7 BIBLIOGRAPHY 47

8 ANNEX I – INTERVIEW QUESTIONS 53

9 ANNEX II – SURVEY 54

10 ANNEX III: PHONE INTERVIEW WITH THE JUSTICE DEPARTMENT 57

11 ANNEX IV: KEY FINDINGS FROM THE NIS DIRECTIVE IMPACT ASSESSMENT 58

List of abbreviations

EU	European Union
EEA	European Economic Area
NISD	NIS Directive
GDPR	General Data Protection Regulation
ECHR	European Convention on Human Rights
TFEU	Treaty on the Functioning of the European Union
AU Convention	The African Union's Convention on Cyber Security and Personal Data Protection
CoE	Council of Europe
Cybercrime Convention	Budapest Convention on Cybercrime
GRC	Governance, Risk and Compliance
TRS	Technical Risk Services
NISD Impact Assessment	Commission Staff Working Document Impact Assessment Accompanying the proposal for the NIS Directive
CIS	Critical Information Systems
ISSP	Information System Security Policy
ISMS	Information Security Management System
ENISA	European Union Agency for Cybersecurity
CSIRT	Computer Security Incident Response Team

1 Introduction

Digitalization has opened new possibilities for, for instance, efficiency gains and customer intimacy in the private sector and more efficient and personalized welfare in the public sector, but also an increased risk of cyber related incidents.[1] Cyberspace is a domain of international significance extending far beyond the domain of internal affairs of any state, affecting public safety, economic development and national security, and it is necessary to identify, interpret and apply relevant legal rules to it.[2] Cyberattacks[3] can have a negative effect on several human rights, such as everyone's right for private and family life, as it often will result in the leakage of personal data, for the freedom of expressing and receiving information online[4]. Kubo Mačák argues that many states are reluctant or negative to committing to the application of international law to cyberspace which eventually can create an *opinio juris.*[5] Consequently, if states are not committing to create binding rules, cyberspace is not regulated, and states can act more freely in this sphere.[6] International law has so far not played an important role in policy discussions on cybersecurity and has not been much involved in the global dissemination of the Internet.[7] However, pre-cyber international law principles has been applied to mitigate the threat landscape of today.[8] Prohibition on intervention, use of force, and attacks on civilian targets in armed conflicts are examples of such principles applied to protect critical infrastructure from cyberattacks.[9]

Critical infrastructure[10] is particularly important to protect, as disruption could cause inconvenience and financial losses to the society, such as when trading in the Emissions Trading

[1] (Tabrizi, Lam, Girard, & Irvin, 2019), (The Norwegian Board of Technology, 2017), (ESI ThoughtLab, 2019)

[2] (Mačák, 2016)

[3] (Schmitt, 2013, s. 92): "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"

[4] ECHR Art. 8, NISD Recital 63, ECHR Art. 10. See (Council of Europe, 2020)

[5] (Mačák, 2016). International customary rules are the result of two elements: an established, widespread, and consistent practice on the part of states; and a physiological element known as opinio juris (Evans, 2014, s. 98). Opinio juris is:"evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it" (North Sea Continental Shelf, 1969).

[6] (S.S. Lotus (France v. Turkey), 1927) lays down the concept in which a State can act freely unless the action is prohibited by a contrary international rule.

[7] (Fidler, 2015, s. 10)

[8] Ibid.

[9] (Schmitt, 2013)

[10] A term that will be discussed in Section 3.1

System was suspended by the European Commission in 2011 due to security breaches at national registries, which prevented companies from buying and selling allowances within the European Union (hereinafter referred to as EU).[11] The destruction or incapacitation of such infrastructures could eliminate the states' capability of protecting itself from external threats, resulting in social unrest, significant economic harm, and even loss of life.[12] Protecting infrastructures is a duty of any sovereign state, which requires protecting the security of network and information systems, by implementing measures such as exchange of information, cooperation, common minimum capacity building and planning requirements, and common security requirements.[13]

In Europe, the EU has traditionally been hampered in its attempts to regulate cybersecurity due to its limited competence on internal security.[14] Council of Europe (hereinafter referred to as CoE) was the most important player in establishing a common framework on cybersecurity in the EU, and its Budapest Convention on Cybercrime (hereinafter referred to as Budapest Convention) was the leading treaty in this field. Budapest Convention aimed to harmonise domestic cyber-crime legislation, provide law enforcement with the necessary powers to investigate and prosecute crimes relating to computer systems, and establish an effective regime for international cooperation.[15] The Convention codifies illegal access and interceptions of computer systems, data- and system interference, and misuse of devices, as criminal offences[16]. The implementation of security measures is described as the most effective method of preventing unauthorised access.[17] Similar rules on offences relating to unauthorized access to computers, information theft, and disruption of operations are also adopted in Africa.[18] The fact that existing security tools and procedures were not sufficiently developed or common in the EU, made it necessary to develop a comprehensive regulation at Union level, concerning the security of network and information systems.[19] The EU filled this vacuum by implementing the

[11] (European Commission, 2011)

[12] (Haber & Zarsky, 2017, s. 516)

[13] Ibid. and NIS Directive Recital 6.

[14] TFEU Art. 72 codifies the limitation on EU competence, which forces the EU to respect each individual State's national security.

[15] (Council of Europe, 2001)

[16] Ibid. Art. 2, 3, 4, 5, 6

[17] (Council of Europe, 2001, s. 9)

[18] (African Union, 2014)

[19] (Markopoulou, Papakonstantinou, & de Hert, 2019)

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter referred to as NISD), which is the first piece of EU-wide legislation on cybersecurity.[20] The Directive stipulates the EU to be most capable of achieving a high common level of security in the region, and assigns the responsibility largely on operators of essential services and digital service providers by imposing security requirements.[21]

1.1 Research question

This thesis is mainly focusing on European security requirements imposed on operators of essential services (hereinafter referred to as OES) and digital service providers (DSP) derived from NISD. The analysis of security requirements includes to assess which actors that are subject to the security requirements, what the legal content of the requirements are, how they have been implemented, and to which extent the requirements are consistent across the Union.

The aim of this thesis is to try answering the following question:

To what extent does the implementation of security measures established by the NIS Directive align with the purpose of achieving a high common level of security of network and information systems in the EU?

The thesis applies doctrinal legal and technical research.

To achieve this essential aim, the following sub-questions will be explored:

1. Which actors are subject to NISD? How does the implementation of the Directive in EU countries compare to each other in terms of identifying these actors?
2. Which legal implications follow with the implementation of security requirements?
3. How does the implementation of security requirements in the EU countries compare to each other in terms of the wording of the legislation?
4. Which role does guidelines, recommendations, voluntary industry standards and "state of the art" play for the interpretation of security requirements provided by the Directive?

[20] (Georgieva, 2016)

[21] NISD Recital 74, 44

1.2 Methodology

The research will apply a three-step normativist analysis[22], which will be further elaborated by systematically clarifying and analysing existing law. Judicial policy considerations will also be part of the thesis, which will take into account the implications cybersecurity requirements have on EU countries and organisations within the region. The thesis explores its research questions by interpreting legal sources, administrative practice, national implementation and by the conduction of in-depth interviews and a survey.

The identification and interpretation of security measures is mainly based on legislation derived from European community law in general, and more specific NISD including its Recital. The Recital is an important interpretative tool to explain the purpose and intent with the articles of the Directive.[23] However, the Recital does not have an individual legal basis constituting a binding legal force.[24] The preparatory works (travaux préparatoires) will demonstrate the intention behind the EU legislation, but does only have limited influence on the interpretation. Where relevant, I will also include impact assessments, and national strategies in various EU Member States. Other EU regulations, such as Regulation (EU) 2016/679 of the European Parliament and of 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 (hereinafter referred to as GDPR), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter referred to as ePrivacy Directive), and Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter referred to as eIDas Regulation) are also relevant for the interpretation of the NIS Directive, as the wording and structure of security requirements has many similarities.

[22] The normativist model describes the set of rules that belong to a legal system and its further systematization, by identifying, interpreting and testing the validity of the norms. See (Vaquero, 2013) Section 2.1, paragraph 30, 32, 36.

[23] (Baratta, 2014)

[24] Ibid. See (Judgment of the Court (Fifth Chamber) of 19 November 1998. - Criminal proceedings against Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn, 1998) para. 54.

Rulings by the Court of Justice of the European Union (hereinafter the Court) are also an important legal source for EU law, as it has the power to interpret Treaties and validate and interpret acts of Union institutions.[25] However, in this case, as the Directive has been recently implemented in EU Member States, there are no relevant court decisions. Although analogies to data privacy and technology judgments could be relevant for interpreting the Directive, security requirements are a narrow field in data-related legislations and court decisions on security requirements are therefore not a legal source that will be taken into account. In a few years' time, there would probably be some relevant court cases that could help interpreting the subject of this thesis. In general, court decisions have to be interpreted contextually and in light of the community law as a whole, bearing in mind the state of evolution and objectives.[26] The legal doctrinal research on security requirements provided by NISD will also rely on secondary sources from authorities and relevant doctrine in the academic literature.

In the cyber-specific territory of international law, scholarly works and guidelines play an important role, which should be distinguished from legal norms creating international legal responsibility.[27] For instance, ENISA and NIS Cooperation Group assist and advise on the development and review of EU cybersecurity law, by providing independent opinion and analysis, assist Member States to implement EU cybersecurity law, and specifically issue opinions, guidelines, advise and best practices between competent authorities for the implementation of the NIS Directive.[28] However, there are a vast amount of guidelines available, and it is therefore difficult to assess which guidelines that are best suited to interpret the Directive. I have therefore taken into account some guidelines from EU agencies, as they probably are used by national competent authorities (NCA) in their compliance assessments.

The NIS Directive permits the Member States the flexibility in how to implement the legislation, which makes it valuable to systematically analyse the legislative processes of national transpositions, and examine the commonalities and differences, patterns and methods. Most of these sources are written in the local language, and as the assessment of national transpositions necessitates to apply online translator services for the translation of local language to

[25] TFEU Art. 267

[26] (Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health. - Reference for a preliminary ruling: Corte suprema di Cassazione - Italy. - Obligation to request a preliminary ruling, 1982)

[27] (International Law Commission, 2001) Art. 1

[28] Regulation (EU) 2019/881 Art. 5 (1) and (2), and NISD Recital 66

English, it would probably be somewhat inadequate to establish the national legal regime. The analysis of the substantive content of the NIS Directive combined with the implementation effort will test the validity and effectiveness of the norms in relation to its capability to align with the purpose of the Directive. However, the quality of the assessment would have been better if the local edition was supported by an edition in English.

Implementation of security requirements precondition not only legal considerations, but also a highly technical exercise, including organisational, procedural and technological aspects. Thus, an understanding of implementation in practice is relevant. In addition to the legal interpretation, the thesis also comprise in-depth interviews with three senior security leaders from the leading cybersecurity company in the Nordics, mnemonic AS, and a survey conducted among 17 security consultants in the GRC and TRS division from the same company. The company has been chosen as a resource both because I have a working relationship in this firm, and as the company is internationally recognised for offering high quality cybersecurity services. The three employees featured in the in-depth interviews hold numerous cybersecurity-related certifications, have combined over 40 years of cybersecurity experience, and have achieved Master's degrees in fields such as Communication Technology, Computer Security, Computer Engineering, and a PhD in Cryptology. They have been interviewed individually, but as they responded similarly and due to word limit, I have merged their answers. The interview questions are located in Annex I of the thesis. The survey was conducted in December 2019, and the questions and graphs representing the response are located in Annex II. Both the answers from the interviews and statistics from the survey have been spread into the sections which are relevant. I had originally planned to also interview representatives from critical sectors in Europe to provide experiences from outside the cybersecurity industry, but the organisations I approached did not have time to perform interviews.

Finally, I have gathered information on the Norwegian implementation of the NIS Directive by performing an unofficial telephone interview with a senior advisor working in the Justice Department of Norway. The opinions stated by the senior advisor is not representing the official views of the Justice Department, but describes the internal procedures.

1.3 Structure

The thesis comprises of four chapters. The first chapter aims to explain the background, purpose and rationale of the NIS Directive, and provides the legal basis for security requirements in the

EU and the first EU-wide legislative piece on cybersecurity. The second chapter elaborates on the actors covered by the Directive, and a description of the methodological approaches practiced by Member States in the identification of OES in the EU. The third chapter details the content of security requirements, by analysing and comparing the obligations imposed on OES and DSPs, and comparing the requirements to the security requirements in GDPR. The fourth chapter analyses the commonalities and differences in the transposition of the Directive in Member States, and the implementation of security requirements in organisations, by discussing the terms “appropriate”, “proportionate”, “state of the art” and “high common level”, the role of voluntary standards and non-binding recommendations, and reflecting on to what extent the security measures aligns with the purpose of the Directive. This chapter will also discuss whether the actual implementation would lead to disproportionate burdens on companies, and the variations of individual cybersecurity ambitions.

1.4 Demarcations

The thesis will restrict its coverage to discuss the content, context and implementation of security measures towards operators of essential services (hereinafter referred to as OES) and digital service providers (hereinafter referred to as DSP) established by the NIS Directive Art. 14 and 16. However, the thesis will not include notification requirements, network of Computer Security Incident Response Teams (hereinafter referred to as CSIRTs), or national strategies, as the thesis would be too general if also these subjects were to be included. Security and notification requirements are definitely related, as the security level of an OES or DSP requires both to manage risks and to notify when incidents occur. There are many evaluations that has to be addressed for the notification regime, which could be a thesis topic by itself, and the inclusion of notification requirements would result in a broader and more general thesis. [29] NIS Cooperation Group, national competent authorities, requirements imposed on Member States, enforcement and penalties for non-compliance will be discussed on a general level, as these topics are relevant for the interpretation of security requirements in the NIS Directive.

[29] Such as the assessment of what a «substantial impact» constitutes, and the scheme of notifying a competent authority, cf. NISD Art. 16 (3)

2 Brief on NIS Directive security requirements

The European Union has the power to adopt measures to establish or ensure the functioning of the Internal Market, by approximating the law, regulation or administrative practice.[30] The EU has already acknowledged the necessity to harmonise rules on network and information systems to ensure the emergence of the internal market by applying TFEU Art. 114 on security-related EU legislative acts.[31]

2.1 Policy rationale

In areas in which the EU does not have exclusive competence, the principle of subsidiarity has been practiced for the Union to act in cases where the proposed action "cannot be sufficiently achieved by the Member States (…) but can rather, by reason of the scale of the effects of the proposed action be better achieved at the Union level".[32] Prior to the NISD, the voluntarily approach resulted in an uneven playing field where only the minority of high-performing Member States have cooperated with each other, and to ensure cooperation among all Member States, it is necessary to establish a required minimum level of capabilities.[33] Furthermore, the countries' capabilities varied significantly, meaning some invested heavily in security, some had a slower pace, and some with a low level of security spending and maturity.[34] NISD Impact Assessment states in 4.1.5.1 that the lack of security is having a negative impact on the users' trust in the online economy, which threatens the Internal Market. Overall, the level of protection of network and information systems is insufficient across the EU, which results in disruptions to the EU internal market, rising number, frequency and complexity of security incidents, affecting all sectors in the society and economy.[35] Thus, the EU has established rules justified by the principle of subsidiarity due to the cross-border nature of the problem and the improved effectiveness to existing national policies, to protect network and information systems and combine these rules with the adoption of legal devices, such as security measures and notification of breaches to a supervisory authority and to the public.[36] Without the implementation of common EU security measures, the Member States would act on their own – which could reduce EU's

[30] TFEU Art. 26 and 114

[31] Regulation (EU) 2019/881, and Directive (EU) 2015/1535 both refers to TFEU Art. 114.

[32] Treaty on European Union Article 5. See also (European Commission, 2008)

[33] (European Commission, 2013) 5.4.2

[34] Ibid. 4.2.1. The Impact Assessment refers to a market study, pointing out that the countries with the highest GDP spent 82% of the total security spending.

[35] (European Commission, 2013) par. 4

[36] Ibid. 5.4.2 and (Porcedda, 2018, s. 2)

role in international scene.[37] The rationale for implementing the Directive is that the "existing capabilities are not sufficient to ensure a high level of security" as the levels of preparedness differs very between Member States, which has resulted in fragmented approaches in the Union.[38] The absence of common requirements on OES and DSPs[39] makes it impossible to establish an effective and global cooperation mechanism among Member States.[40] NISD provides legal measures to boost the level of cybersecurity in the EU, and has three main objectives: improving national cybersecurity capabilities, building cooperation at EU level, and promoting a culture of risk management and incident reporting[41]. According to NISD Recital 74, the Union is permitted to adopt measures in accordance with the principle of subsidiarity, and not go beyond the principle of proportionality.

2.2 Background and purpose

The NIS Directive is secondary EU law, which is binding, but it is up to each Member State to choose the form and methods of the implementation.[42] This is contrary to GDPR, which is a regulation. A regulation is binding in its entirety and shall be directly applicable in all Member States.[43] Secondary law is hierarchical below EU treaties, such as the Treaty of the Functioning of the European Union (TFEU) and general principle of EU law, such as fundamental rights.

Network and information systems are considered an essential element for the smooth function of the cross-border movement of goods, services and people, and significant disruptions can affect both individual Member States, and the Union as a whole.[44]

The purpose of the Directive is to achieve a "high common level of security of network and information systems in the Union".[45] The Directive is a minimum harmonisation directive, meaning that the directive establishes minimum standards, allowing the EU countries to impose

[37] (European Commission, 2013) 4.1.5.3

[38] NISD Recital 5

[39] I refer to DSPs instead of DSP when I talk about more than one digital service provider.

[40] Ibid.

[41] Ibid. and (European Commission, 2017)

[42] TEU Art. 189 (3)

[43] TEU Art. 189 (2)

[44] NISD Recital 3

[45] NISD Recital 74

stricter obligations.[46] However, Member States are strongly discouraged to impose stricter requirements on DSPs, which will be discussed later in this thesis. The Directive is two-sided, and applies both towards Member States and OES/DSP, but with different responsibilities.[47] As this thesis is focusing on security requirements, the latter category will be most relevant[48].

To mitigate security challenges on network and information systems requires common minimum capacity building and planning requirements, cooperation, exchange of information, and common security requirements for OES and DSP across the Union.[49]

Network and information system is defined as either an electronic communications network, any interconnected or related devices performing automatic processing of digital data, or digital data which is stored, processed, retrieved or transmitted to operate, use, protect or maintain one of the two other elements. [50] The security of such systems is the ability to resist any action that will compromise "the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems".[51]

The Directive aims to promote a culture of risk management, in which risk is defined as "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems".[52]

With the exception of NISD Art. 1 (2) d), the main obligations for Member States are stipulated in NISD Art. 1 (2). Member States may adopt further obligations with an ambition on achieving a higher level of security of network and information systems, but this is voluntary.[53] In other

[46] NISD Art. 3 See (European Commission, 2018)

[47] NISD Recital 7

[48] As security requirements are imposed directly on OES and DSP, cf. NISD Art. 1 (2) d)

[49] NISD Recital 6

[50] "Electronic communications network" within the meaning of Directive 2002/21/EC Art. 2 point (a). Definition is stipulated in NISD Art. 4 (1).

[51] NISD Art. 4 (2). (Nieles, Dempsey, & Pillitteri, 2017): "Confidentiality: preserving authorized restrictions on information access and disclosure. Integrity: Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. Availability: Ensuring timely and reliable access to and use of information."

[52] Risk management: NISD Recital 4. Risk definition: NISD Art. 4 (9)

[53] NISD Art. 3. See: (Baratta, 2014)

words, mitigating security challenges on network and information systems requires a culture of risk management, in which the Directive stipulates common security requirements on OES and DSP, which will allow the maintenance of a functioning Internal Market. However, the creation of a high common level of security across the Union also depends on other factors, which will be discussed at a later stage.

2.3 The EU regulatory landscape of cybersecurity requirements

Prior to the NIS Directive, there were loopholes in the regulatory framework, as only the electronic communications sector, identity assurance services and trust providers, and to some extent payment service providers were imposed obligations to perform risk management and notify serious incidents[54]. The adoption of GDPR**,** which took place the same year as NISD, imposes obligations on data processors and data controllers, including critical sectors such as banks, hospitals etc., to implement appropriate and proportionate security measures.[55] However, the security requirements are only related to the processing of personal data.[56]

Council Directive 2008/114/EC stipulates an obligation for Member States to identify potential European Critical Infrastructures and to implement security plans, but does neither require these entities to report significant breaches nor entail rules for cooperation and incidents response by Member States. Only a few organisations have been identified as European Critical Infrastructure.

[54] (European Commission, 2013) 5.1., (European Commission, 2002), (European Commission, 2014), (Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, 2015)

[55] GDPR Art. 32

[56] Ibid.

3 Actors subject to the Directive

The Directive is applicable for the EU Member States, OES and DSPs[57]. Public communication networks, publicly available electronic communication services and trust providers are not subject to the obligations on OES and DSP[58]. The Union law for the Eurosystem's oversight of payment and settlement systems are not affected by the Directive.[59]

3.1 Operators of essential services (OES)

Member States shall identify OES, and establish a list of services which should serve as a reference point in the identification of OES.[60] The list should be updated on a regular basis.[61]

An OES is a public or private entity which is *essential* for the maintenance of critical societal and/or economic activities, and is *dependent* on network and information systems.[62] A potential incident affecting this entity has to result in *significant disruptive effects* on service delivery[63]. The criteria are cumulative, meaning that all of them has to be satisfied in order for the entity to be considered an OES.

Firstly, whether the service is essential has to be assessed by the Member State, and the Directive consider it sufficient to evaluate if the potential OES provides services that are included in the list of essential services.[64] Typical examples of essential services are provided in Annex II:

- energy (sub-sectors: electricity, oil and gas),
- transport (sub-sectors: air transport, rail transport, water transport and road transport), banking,

[57] NIS Directive Art. 5 and 7 establishes, for instance, the Member States' responsibility to identify OES within their jurisdiction, and adopt a strategy ensuring a high level of security. NISD Recital 7 establishes the Directive's applicability towards OES and DSP. (European Commission, 2013) 4.14 provides rationale for the choosing of critical sectors in NISD.

[58] (European Commission, 2002) defines electronic communication services, and specifies security and integrity requirements imposed in Art. 13 and 13b. Regulation (EU) No 910/2014 defines trust providers and the specific security requirements applicable to them are regulated in Art. 19. NISD Recital 7 and Art. 1 (3) stipulates the actors not subject to the Directive.

[59] NISD Recital 14 referring to (OPINION OF THE EUROPEAN CENTRAL BANK of 25 July 2014 on a proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 2014)

[60] NISD Art. 5 (1), (3), Recital 23

[61] NISD Art. 5 (5)

[62] NISD Art. 4 (4) defines an operator of essential services (OES) and refers to the criteria laid down in Art. 5 (2).

[63] Ibid.

[64] NISD Recital 20

- financial market infrastructures,
- health sector,
- drinking water supply and distribution, and
- digital infrastructure.

Member States have used prior experience, such as national provisions on “vital operators”, or Council Directive 2008/114/EC on critical infrastructures to establish a methodology[65]. The Council Directive defines critical infrastructure in Article 2 (a), which elaborates the range of essential in categories of maintaining vital societal functions, safety, health, economic or social well-being of people and security. Comparing the term critical infrastructure with other jurisdictions provides some interesting findings. In the U.S. critical infrastructure covers all vital physical or virtual systems or assets, while it is more specific to network facilities in China[66]. Conversely, “grunnleggende nasjonale funksjoner” in the Norwegian Security Act covers many types of activity, but restricts its threshold to only cases where the whole or partial loss of function would impact the ability to safeguard national security interests, which probably sets the bar higher than in the U.S., China and in Europe. [67]

However, the NIS Directive permits Member States to go beyond the scope of Annex II and include additional services and sectors.[68]

Secondly, that essential services depends on network and information systems is a criterion many EU countries consider given in today’s society, but the Directive requires Member States to demonstrate the dependency.[69]

Thirdly, the incident affecting the critical sector must result in a significant disruptive effects, which is codified in NISD Art. 6. The article provides a non-exhaustive list of cross-sectoral factors that should be taken into account when considering if the incident has significant disruptive effects, such as:

- the number of users relying on the service,
- the dependency between the potential essential service and other essential services,
- the impact that incidents could have,

[65] (European Commission, 2013)

[66] U.S: defined in (U.S. Congress, 2001). NIST cybersecurity framework applies this definition for securing cybersecurity of critical infrastructure. China: (China Cyber Security Coordination Bureau, 2017)

[67] (Justis- og beredskapsdepartementet, 2018) §1-5 (2)

[68] NISD Recital 23, and (European Commission, 2019) The purpose of the report is to reduce the risks related to cross-border dependencies, different interpretations of the Directive, safeguard a playing level field for OES in the Internal Market, and to develop a comprehensive overview of cyber-resilience level in the Union.

[69] NISD Recital 20 and (European Commission, 2019)

- the market share of the entity,
- the geographic spread of an incident,
- and the importance of the entity for maintaining a sufficient level of the service.

NISD Art. 6 (2) establishes that sector-specific factors should be considered in addition to cross-sectoral factors, which is further exemplified in NISD Recital 28.

The purpose to achieve a high *common* level of security requires a consistent approach on identification of OES, and Member States are supported by the NIS Cooperation Group in taking such an approach.[70] To ensure such consistency, the EU countries shall submit necessary information, including the list of services of essential services, national measures for identifying OES, number of OES in the Member State, and thresholds as a minimum.[71]

The recent EU report on methodologies, published in October 2019, is a result of such submitted *necessary information*, illustrating that the methodologies used by Member States differentiates significantly in the Union, including which authorities that shall identify, assessments of the dependence of network and information systems, the definition of OES and the application of thresholds.[72]

The degree to which the identification process is centralised varies between EU countries, but the most common practice is to delegate some of the process to sectoral authorities, and that a single authority has the responsibility to provide guidance to sectoral authorities.[73] Such practice could seem logical as usually sectoral authorities understand their sub-sectors better than the main authority. Nonetheless, some countries have delegated the whole identification process to a single authority, and in the most extreme cases sectoral authorities develop their own methodologies. The report claims that some argue that centralised identification leads to less reluctance from OES, as there is a fear of repercussions when sectoral authorities has the role to identify.[74]

The identification process varies between a top-down approach, in which public authorities performs the identification process, and a bottom-up identification, in which operators can verify themselves whether they satisfy the requirements as OES or not.[75] Although most cases seems to be top-down, the authorities are dependent on some self-assessment exercises from

[70] NISD Art. 5 (6) and 11 (3) l

[71] Cf. NISD Art. 5 (7) a)-d)

[72] (European Commission, 2019)

[73] Ibid.

[74] Ibid.

[75] Ibid.

the potential OES. Such practice seems reasonable as it demands less resources from the authorities, which could be important in an industry with lack of skilled competence.[76]
Part of the identification process requires the EU countries to assess the OES' dependence on network and information systems, and in practice this varies between those countries conducting detailed assessments, while others refer to the potential OES to self-assess their dependence[77].

EU countries are required to consult each other before the decision is made on the identification of OES providing services in more than one EU country.[78] Experiences from the EU report illustrates that only a few Member States have chosen to consult other Member States, due to lack of secure channels, delayed identification processes, and the significant amount of cross-border dependencies.[79]

3.1.1 Consistency differences

The number of identified services varies between both between Member States as a whole, but also on the amount of individual entities in each sector, which corresponds with the degree of granularity across the Union.[80]

The figures below are excerpts from the mentioned EU report. The European Commission applies the terminology "consistency gaps", which could be misleading. As the Directive entails minimum harmonisation, the Member States are free to identify its essential sectors independently. Thus, demonstrating differences in methodological approaches on identifying sub-sectors within sectors should not be considered "consistency gaps", but "consistency differences", as a "gap" constitutes a break in continuity, which is not evident in this case as it is up to each Member State to determine continuity. [81] The figure shows that some countries (Estonia, for instance) have chosen a broad and general definition which opens up the possibility to basically identify any operator in the electricity subsector as OES, while Bulgaria on the other hand identifies OES based on a very detailed list of services, also adding a sector outside Annex II to its list. The report suggests that consistency differences are a result of the different

[76] (Crumpler & Lewis, 2019)

[77] (European Commission, 2019)

[78] NISD Art. 5 (4). (NIS Cooperation Group, 2018) provides guidance for conducting cross-border consultations

[79] (European Commission, 2019)

[80] Member States have on average identified 35 services per State, and the number of identified services ranges from 12 to 87. Source: (European Commission, 2019)

[81] (Merriam-Webster, 2019)

implementation of the Directive and the minimum harmonisation approach, but underlines that differences in identification does not entail that Member States have implemented the Directive incorrectly.[82]

Consistency differences in the definition of OES			
Estonia (least granular approach)	**Portugal**	**Denmark**	**Bulgaria (most granular approach)**
Electricity supply	Distribution system operators	Electricity Distribution	Distribution of electricity
*	*	*	Ensuring the functioning and maintenance of a distribution system for electrical energy
*	Transmission system operator	Electricity Transmission	Transmission of electricity
*	*	*	Operation, maintenance and development of an electricity transmission system
*	*	Electricity Production	Electricity production
*	*	*	Electricity Market

* Consistency differences

The thresholds for identifying OES also varies greatly between Member States, both qualitatively and quantitatively.[83] Thresholds are applied differently across the Union, and can be based on a single quantitative factor, e.g. the numbers of systems supporting the service, a larger set of quantitative factors, e.g. the numbers of systems plus the market share, or a combination of quantitative and qualitative factors.[84]

[82] (European Commission, 2019)

[83] Ibid.

[84] Ibid.

Threshold differences			
Country	**Internet Exchange Points (IXP)**	**DNS providers**	**Top-Level-Domain registries**
Sector-specific thresholds			
Austria	connected autonomous systems > 100	DNS resolvers: 88 000 users; Author. DNS: 50 000 domains	50 000 domains
Germany	connected autonomous systems > 300	DNS resolvers: 100 000 users; Author. DNS: 250 000 domains	(service not identified)
Denmark	av. daily data volume > 200 gbit/s	DNS resolvers: 100 000 users; Author. DNS: 100 000 domains	500 000 domains
Malta	25% of market share	DNS resolvers: 78 000 requests/day; Author. DNS: 7 800 domains	750 000 requests/day
United Kingdom	market share > 50%, or interconnectivity to global internet routes ≥ 50%	DNS resolvers: 2 000 000 clients/day; Author. DNS: 250 000 domains	TLD registries ≥ 2 billion queries/day
Cross-sectoral thresholds			
Cyprus	50 000 users, or 5% of subscribers of the market	50 000 users, or 5% of subscribers of the market	50 000 users, or 5% of subscribers of the market
Lithuania	inhabitants > 145 000	inhabitants > 145 000	inhabitants > 145 000

11 out of 28 Member States have identified OES outside the scope of the Annex II, and the next two figures illustrates additional and excluded sectors.[85]

Country	**Other sectors classified as OES in addition to Annex II[86]:**
Austria	Public administration
Cyprus	Electronic communications, wastewater, food, government and national security / emergency services and environmental services.
Estonia	Electronic communication service providers, public broadcasting, providers of digital identification and digital signing service and district heating service providers.
Czech Republic	Chemical industry.
Finland	DSPs (online marketplaces, search engines and cloud providers) and other digital infrastructures.
France	Industries involved in the civil activities of the state, judicial activities, military activities of the state, food, electronic, audio-visual and information communication, space and research, and finance industries.
Lithuania	Industrial sector, chemical and nuclear sub-sector, state administration, civil safety, environmental, national defence and foreign and security affairs.
Poland	Heating and mining sub-sectors.
Portugal	Critical infrastructures and public administration as part of the scope for the jurisdictional oversight of the cybersecurity authority; however, the OES requirements are not applicable.
Slovakia	Pharmaceutical/chemical/metallurgical industry, security, public administration information systems, defence, intelligence services, classified information, electronic communication/satellite communication, networks and services of fixed and mobile electronic communications, and postal service.
Slovenia	Environmental protection industries.

[85] Ibid.

[86] Based on (European Cyber Security Organisation & DigitalEurope, 2019)

Country	**Changed or excluded Annex II-sectors**[87]
Latvia	Does not specifically exclude the banking and financial market infrastructures as OES, but refers these sectors to sector-specific legislation and requirements (lex specialis).
Netherlands	Has excluded the health sector as OES.
Slovakia	Slovakian legislation has changed the sectors relating to Annex II.

3.1.2 Considerations and discussion

The in-depth interviews conducted among cybersecurity leaders suggest that assessing which actors that are subject to the Directive is one of the most important phases for achieving a high common level of security. However, they think the criteria are difficult to assess, such as *essential, dependent and significant disruptive effects*, as the criteria can be too vague, and can unintentionally collide with other similar legislations and create overlaps. Thus, essential sectors need predictable rules on identification. The definition in NISD Art. 5 (2) provides clear cumulative criteria for defining an organisation as an OES, and is precise on taking a consistent approach, but does not provide a legal requirement on Member States to apply any specific definitions and thresholds consistently.[88] Experiences from the past two years illustrates methodological inconsistencies which the cybersecurity leaders fear could lead to an uneven playing field between OES across the Union, with possible implications on the functioning of the Internal Market, and contradict the purpose of the Directive. Thus, one can question if the purpose of the Directive (to achieve a high *common* level of security) is safeguarded with such varying practices in the identification of one of the main actors, OES, and if the Directive should have required Member States to only use a defined set of methodologies, thresholds or list of actors that could constitute OES. I would not consider the inconsistency by defining OES as other sectors than provided in Annex II as problematic in itself, as different countries may have different business environments in different sizes, but the purpose of stipulating a *common* level of security is definitely confronted. Thus, what is *common* if the actors and the methodologies

[87] Ibid.

[88] See (European Commission, 2017, s. 5)

to identify the actors are different across the Union? The European Commission also supports this view, as the report concludes that the identification process in the EU is significantly fragmented, due to how the Directive has been designed and how Member States have implemented methodologies.[89]

The cybersecurity leaders state that the variations of definitions could be problematic, as they create consistency differences, but also necessary for some countries. Conversely, thresholds and the possibility to add sectors outside Annex II can and should be different – as countries have unique characteristics and challenges.

3.2 Digital service providers (DSP)

Digital service providers (DSP) offers services often supporting OES, and are defined as "any legal person that provides a digital service", which is of a type listed in NISD Annex III[90].
A "digital service" means "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".[91] Types of DSPs detailed in Annex III are online marketplaces, online search engines and cloud computing services. An online marketplace is the final destination for the conclusion of online sales or service contracts between consumers and traders, but does not cover online services acting as an intermediary to a third-party in which the contract would be concluded, or price comparing services.[92] An online search engine is a platform where the user can search all websites on the basis of a query on a subject, but does not cover the search functions limited to a specific website, or price comparing services.[93] Cloud computing services includes services that "allow access to a scalable and elastic pool of shareable computing resources", including storage, applications, networks, servers or other infrastructure and services.[94] "Scalable" is understood as computing resources which the cloud service provider has allocated flexibly, regardless of where the resources are physically located. "Elastic pool" describes the computing resources' ability to increase and decrease its resources quickly based on the workload. "Shareable" means

[89] (European Commission, 2019)

[90] NISD Art. 4 (6), cf. NISD Art. 4 (5)

[91] Defined in Directive (EU) 2015/1535 Art. 1 (1) b). Further guidance for clarifying the definition in Art. 1 (1) b) is provided in its (i)-(iii)

[92] Defined in NISD Recital 15

[93] Defined in NISD Recital 16

[94] Defined in NISD Recital 17

that multiple users with a common access share the computing resources, but the processing is initiated for each unique user from the same electronic equipment.[95]

Online marketplaces and search engines are somewhat easier to define than cloud computing services, as the latter category is vast and can include cloud services deployed as an infrastructure (IaaS), as a platform (PaaS), or as a software (SaaS).[96] The model of shared responsibility often practiced by cloud computing services makes it even more difficult to assess which areas of the network and information systems the DSP is responsible for, and what the customers need to secure themselves.[97] Usually, the contracts cover such risk transitions.

Member States are not required to identify DSPs, in which guarantees a catch-all-approach, and in which the DSP has to self-assess whether the provider should comply with the Directive or not.[98] Thus, this assessment suggests that the potential DSP has knowledge of its risks and vulnerabilities exposure, which indicates that a risk analysis probably has to be performed anyway. The Member State where the DSP has its main establishment and head office is the country which has jurisdiction. [99] In cases where an DSP offering Annex III-related services is not established in the Union, the DSP shall designate a representative in the Member State where the services are offered, which will be subject to that particular Member State's jurisdiction.[100] However, micro- and small enterprises are excluded to adopt security requirements, to avoid imposing a disproportionate burden on companies which does not have the same amount of risk posed to its network and information systems.[101]

Experiences since the Directive was implemented in the EU suggests that all countries have harmonised the classification of DSPs as the three sectors provided in Annex III, expect Finland including all DSPs as OES.[102] However, although the rules on jurisdiction and territoriality is applied similarly across the Union, there are some exceptions on registration requirements.[103] The scheme of how the different registration requirements are functioning in practice

[95] Ibid.

[96] See (Finnish Transport and Communications Agency - National Cyber Security Centre, 2020) and (Ireland National Cyber Security Centre, 2019)

[97] (Cloud Security Alliance, 2017)

[98] NISD Recital 57. See (Markopoulou, Papakonstantinou, & de Hert, 2019)

[99] NISD Art. 18 (1) and (2)

[100] Ibid.

[101] Cf. NISD Recital 53, Art. 16 (11). See definition of micro- and small enterprises in (European Commission, 2003). (European Commission, 2013) 4.1.4 for the NISD provides rationale. See also NISD Recital 53

[102] (European Cyber Security Organisation & DigitalEurope, 2019)

[103] NISD Art. 18

are not specified yet in all national legislations, but I have found that the main differences consists of two categories. Most of the countries require the same criteria as the Directive entails, while some require the DSPs to register with the authority within the first 30 days (Slovakia and Slovenia) or 3 months (United Kingdom) of operations in that country.

One can argue that it is problematic that DSPs determine themselves if they are considered DSP or not, and that the supervisory obligation from the Member State only will be initiated ex post, which reduces the regulatory pressure towards DSPs significantly. However, it is important to not impose disproportionate burdens on companies.

4 The content of security requirements

4.1 Security requirements are part of culture of risk management

Common security requirements for OES and DSP are one of the central measures to respond effectively to the challenges of the security of network and information systems, and the responsibilities in ensuring such security lies, to a great extent, on OES and DSP[104]. The implementation of security measures appropriate to the risks faced and risk assessments are part of what the Directive constitutes as a "culture of risk management", and such risk management involve measures to "identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact"[105]. Both OES and DSPs shall identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems.[106] In the process of implementing appropriate and proportionate technical and organisational measures, they shall have in regard the state of the art and ensure a level of security appropriate to the risk.[107] Preventing and minimising the impact of incidents also requires an implementation of appropriate measures.[108] Security requirements applies to OES and DSP regardless of if the network and information systems are managed internally or has been outsourced.[109] OES and DSP can implement stricter security requirements than those provided under the NISD.[110]

[104] NISD Recital 6, cf. NISD Recital 44

[105] NISD Recital 46

[106] NISD Art. 14 (1), and 16 (1)

[107] Ibid.

[108] NISD Art. 14 (2), and 16 (2)

[109] NISD Recital 52

[110] NISD Recital 6

The Directive differentiates between OES and DSP, in which stricter requirements are imposed on OES and lighter and more harmonised requirements can be imposed on DSP.[111] Many of the NISD main articles describes these differences, and the lighter approach towards DSP is justified in its less essential service delivery (compared to the service OES provide).[112] The Directive stipulates that further national security measures should apply for OES and not for DSP, which is exemplified in OES' responsibility to notify competent authorities even in cases where the OES depends on a third party DSP.[113]

The survey performed among security professionals illustrates that strict security requirements on OES are considered essential or very important. In the case of DSPs, the results are not the same, although it has very similar results. The service OES deliver is more critical, which can explain why the results were not identical. Accordingly, there is a strong opinion on the role of security requirements as a tool for organisations to maintain a high common level of security.

Art. 1 (7) and Recital 9 stipulates the principle of lex specialis, meaning that sector-specific EU legal acts imposing at least equivalent security requirements will override the NISD.[114]

I will in the following evaluate the different security requirements imposed on OES and DSPs.

4.2 Security requirements imposed on OES

OES are only subject to specific security requirements for the essential part of their service, which excludes the non-essential operations, as the main objective of these security requirements is to ensure continuity of deliverance of essential services.[115] For instance, a company within the energy sector would have to comply with the security requirements in its network and information systems supporting the energy production and distribution, but the headquarters with mainly business functions is not necessarily subject to security requirements derived from the Directive. However, such evaluations would depend on the dependencies between the IT and OT networks, in which the latter is the operational network supporting the industrial control systems. The implementation and enforcement of security requirements imposed on

[111] NISD Recital 57 and 49

[112] (Markopoulou, Papakonstantinou, & de Hert, 2019, s. 6 and 7)

[113] (Markopoulou, Papakonstantinou, & de Hert, 2019, s. 6). See NISD Art. 16 (5).

[114] Exemplified with the water transport sector in NISD Recital 10.

[115] (Markopoulou, Papakonstantinou, & de Hert, 2019). NISD Recital 22.

OES requires the Member States to make sure competent authorities are capable of assessing the compliance of OES derived from NISD Art. 14; and capable of requiring information necessary through security policies and evidence of effective implementation of these policies through a security audit[116]. The potential lacks of compliance documented by the security audit may lead to binding instructions provided by the competent authority.[117] The survey indicate that over 70% of the recipients think that the national competent authority plays an essential or very important role for assessing the compliance of OES. The rest considered it moderately important, and a few considered it slightly important. The question did however neither mention alternatives, such as private companies performing compliance assessments instead of public authorities, nor if it is "important" or if it actually works as intended in practice. This could also explain why the recipients could choose other categories due to the lack of other options. Conversely, the recipients could also think the compliance assessments are not that important.

The Commission encourages Member States to follow the NIS Cooperation Group Reference Document to align the national provisions to the greatest extent possible.[118] According to the NIS Cooperation Group Reference Document, Member States should take into account some general principles for the implementation of security requirements[119]. Some of the recommendations from NIS Cooperation Group Reference Document will be mentioned later in the thesis.

ENISA provides advice and guidelines in information security, and their guidelines on "mapping of OES security requirements to specific sectors" is a comprehensive sector-specific framework OES can apply to ensure an appropriate level of security.[120] The report is based on desktop research of international information security standards, guidelines and good practices

[116] NISD Art. 15. Member States' obligation to designate competent authorities, single points of contact and CSIRTs are stipulated in NISD Art. 1 (2) e). NISD Art. 15 (1), cf. 15 (2) a) and b)

[117] NISD Art. 15 (3)

[118] (European Commission, 2017)

[119] The Cooperation Group, cf. NISD Art. 11, facilitates strategic cooperation between the Member States regarding the security of network and information systems. (NIS Cooperation Group, 2018) provides Member States with a common consensual basis, which describes principles and domains of cybersecurity measures, and promotes a convergent transposition of OES' security measures in Member States. The document page 9, recommends that security measures should increase the cybersecurity of OES in an effective way, tailored to the measures having the most impact on the OES, compatible by addressing common security vulnerabilities of OES, proportionate to the risks, concrete and simple to understand, verifiable, and include all relevant security domains that could participate in strengthening the cybersecurity of OES.

[120] (European Union Agency For Network and Information Security (ENISA), 2017)

which can be applicable for different critical sectors. The report is particularly relevant for establishing a common baseline level of security of network and information systems.

Although the reference document and the Guidelines from ENISA provides guidance in what kind of organisational and technical measures the OES can consider to implement, and which standards that are applicable for the different sectors, they do not reflect legally binding obligations. Neither will they work to establish new standards or duplicating existing ones, but providing a clear and structured image of the current and often common approaches to the security of OES.[121] The mapping of security requirements for the different sectors is a valuable and necessary tool for the entity to implement appropriate and proportionate measures at a baseline level of security. Thus, although the standards and guidelines are non-binding, they will probably be practiced by the NCAs or qualified auditors to ensure compliance, and in cases of non-compliance the NCA has the power to enforce the OES to implement certain security measures. The view of applying internationally recognised standards are also supported by the cybersecurity industry as important, which will be discussed further in Chapter 5.

4.3 Security requirements imposed on DSP

Safeguarding a level of security appropriate to the risk requires the DSP to consider some important elements, and the implemented measures mitigating incidents affecting their service delivery shall ensure the continuity of those services[122]. The Commission shall issue acts to clarify these elements, which resulted in the Implementing Regulation, as the adoption of an additional legislative measure to specify the security requirements was considered essential.[123] Member States are strongly discouraged to impose further requirements on DSPs, except when this is required to safeguard essential state functions.[124] The degree of risk is higher for OES than for DSP, and DSPs should therefore be subject to lighter requirements, and should have the freedom to choose whether to take appropriate measures for managing risks as long as an appropriate level of security is achieved.[125] DSPs are subject to a high level of harmonisation of security and notification requirements across the EU, which would enable an equal treatment

[121] (NIS Cooperation Group, 2018, s. 5)

[122] NISD Art. 16 (1) a)-e), cf. NISD Art. 16 (2)

[123] NISD Art. 16 (8), (European Commission, 2018), (Markopoulou, Papakonstantinou, & de Hert, 2019)

[124] NISD Art. 16 (10), cf. Art. 1 (6)

[125] NISD Recital 49. (European Commission, 2018) has the objective of clarifying rules and further specification of the elements for DSPs in NISD, cf. Art. 1 and Recital 1.

of DSPs in the Union.[126] The DSP has more freedom to conduct business, which is a crucial factor for their success.[127] ENISA has also concluded that the light-touch approach is aiming for the EU to react efficient and swiftly to cybersecurity incidents without overburdening the DSPs.[128] If there is a need for DSPs to increase their security level, such as where public administrations in Member States use digital services provided by DSPs, they should regulate accordingly in contractual obligations.[129]

The implementation and enforcement for DSP deviates from the process with OES, as Member States shall ensure that the competent authority takes action, if necessary, through *ex post* supervisory measures, meaning after non-compliance with the Directive has been provided by evidence by the DSP itself, by another competent authority or by a user.[130] Moreover, the competent authority has no general obligation to supervise DSPs.[131] To perform the *ex post* supervisory entails a competent authority capable of requiring DSP to provide information necessary, such as documented security policies to evaluate the security of network and information systems, and remedy any failure to satisfy the requirements derived from Art. 16.[132] Competent authorities of Member States shall cooperate and assist each other, including exchanging information and initiating supervisory measures in Art. 17 (2), in cases where the DSP is established in several Member States.[133] The survey with security professionals indicates that while the differentiation of OES and DSP is represented by the lack of competent authorities assessing DSP compliance, 64,7% of the respondents think they should have been audited regularly. This is an interesting finding, as the lack of compliance assessments are one of the biggest differences between OES and DSP. However, the recipients were not asked whom to perform such an assessment, and the answer could have been different if they were asked whether *public authorities* should have audited DSPs regularly.

[126] NIS Directive Recital 49 and 57

[127] Ibid.

[128] (European Union Agency for Network and Information Security (ENISA), 2017)

[129] NISD Recital 54 details such scenarios and Recital 56 continues on specific security requirements for public-sector bodies when using cloud computing services

[130] NISD Art. 17 (1), cf. NISD Recital 60. Implementing Regulation Recital 9 describes a user as natural and legal persons who are visiting an online search engine and customers/subscribers to cloud computing services or online marketplaces.

[131] Ibid.

[132] NISD Art. 17 (2) a) and b)

[133] NISD Art. 17 (3)

The Commission Implementing Regulation's objective is to clarify the elements provided in NISD Art. 16 (1) and the parameters in Art. 16 (4). [134] Whether an event is considered substantial will involve the notification requirements imposed on DSP, which is not part of the scope for this thesis. Implementing Regulation Art. 2 is the most relevant article in terms of security requirements for DSP, as it continues on the elements derived from NISD Art. 16 (1) and Recital 69. Implementing Regulation Recital 2 suggests the DSP to use a systematic risk-based approach for the identification of appropriate and proportionate technical and organisational measures.

The element "security of systems and facilities" shall comprise of systematic management of network and information systems, meaning mapping of information systems and establishing appropriate policies in fields like risk analysis, security of operations and security architecture.[135] Physical and environmental security, security of supplies, and administrative security of network and information systems are also important within this category.[136]

The element "incident handling" shall consist of processes and procedures which timely and adequately detects anomalous events, incident reporting and vulnerability identification, adequate response on measures for mitigation, and an evaluation of the scope of incident which includes analysing and collecting information to provide documentation and lessons learnt.[137]

The element "business continuity management" includes maintain or restore the service delivery after a disruptive incident, by creating contingency plans based on business impact analysis, and regularly assess disaster recovery capabilities.[138] The element "monitoring, auditing and testing" requires the DSP to perform an analysis based on a sequence of observations on whether network and information systems functions as intended, verify if the DSP complies with a set of guidelines, and establish processes to expose security faults[139].

Finally, "international standards", refers to which standards that are applicable for security requirements[140].

[134] (European Commission, 2018)

[135] NISD Art. 16 (1) a), cf. Implementing Regulation Recital 4, 5, and 6

[136] Implementing Regulation Recital 7, 8 and Art. 2 (1) d)

[137] NISD Art. 16 (1) b), cf. Implementing Regulation Art. 2 (2) a), b), c), d)

[138] NISD Art. 16 (1) c), Implementing Regulation Art. 2 (3) a), and b)

[139] NISD Art. 16 (1) d), cf. Implementing Regulation Art. 2 (4) a), b), c)

[140] NISD Art. 16 (1) e) "Standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council"

Nevertheless, although the competent authority is only allowed to perform an ex post supervisory, the Implementing Regulation Art. 2 (6) provides the legal obligation for DSPs to verify compliance with the requirements before a potential event occurs. The Implementing Regulation is legally binding in its entirety across the Union, cf. TEU Art. 189 (2). Thus, although the DSP is subject to a light touch ex post supervisory, the security requirements are more streamlined than those requirements imposed on OES.

4.4 Comparing NISD and GDPR security requirements

It is relevant to compare the security requirements in NISD with the GDPR, as the legislations applies much of the same wording, such as "appropriate and proportionate technical and organisational measures". NISD and GDPR were made into law independently without paying much attention to each other.[141] NISD refers to the cooperation between competent authorities and DPAs in cases of personal data compromise caused by security incidents, and GDPR takes account of cybersecurity-related processing[142].

In the case of compliance on security requirements with GDPR and NISD, complying with one legislation does not automatically result in compliance with the other legislation, which means that compliance obligations has to be assessed separately and judged independently.[143] The same applies to the notification regimes under the two legal schemes, as GDPR imposes an obligation to notify in cases of a personal data breach in GDPR, while NISD imposes an obligation to notify in cases of a security incident[144]. In cases of conflict, the GDPR will take precedence, as data protection is a fundamental EU right and therefore a horizontal legal obligation within the EU, while the NISD will be part of national legislation – which is lower in the hierarchy.[145]

The concept of security differs between GDPR and NISD in three ways: purpose and scope of regulations and the role of security, factors that actors have to consider and the degree of detail in the legislation. GDPR is a regulation laying down rules to protect the fundamental rights and protection of personal data, which constitutes a broader scope, as personal data means

[141] Ibid.

[142] (European Commission, 1995), which the GDPR replaced, Art. 2. See NISD Art. 15 (4) and Recital 63. GDPR Recital 49

[143] (Markopoulou, Papakonstantinou, & de Hert, 2019, s. 10)

[144] Ibid., GDPR Art. 33, NISD Art. 14 (3) and 16 (3)

[145] Ibid., TFEU Art. 16 (2) establishes data protection as a fundamental EU right. NISD Recital 75 also refers the Directive to be in accordance with fundamental rights and principles. NISD is to be implemented in national legislation, and GDPR will therefore override – as EU law takes precedence over national law.

any information which can be connected to an identifiable or identified natural person and can consequently impose requirements on everything from tax authorities, to social services, to private healthcare, and to marketing departments for literally any product sold to a targeted group of people[146]. Conversely, the NISD aims to achieve a high common level of security of network and information systems in certain critical sectors. Thus, although the two legislations are fundamentally different, there are also some overlaps. As the processing of personal data often depends on network and information systems, both legislations can be applicable simultaneously[147]. For instance, in some cases data processing of personal data is partially or wholly outsourced to a DSP which is covered by NISD. In other cases, the organisation can both be subject to GDPR as a data controller/processor, but also to NISD as it operates an essential service or offering digital services. Also, the language of GDPR and NISD regarding "appropriate and proportionate technical and organisational measures" are almost identical, which would suggest applying the two regulations analogically for interpretation.

Security can accordingly be described as an implicit purpose of protecting personal data, while NISD consider security itself as the main purpose.[148] More importantly, GDPR does not only provide duties, but also rights for individuals, which makes the regulation a framework both for natural persons to claim their rights and the companies to ensure compliance. The security of network and information systems is on the other hand only providing duties for a few specific sectors which either is identified as OES by the authorities, or consider themselves as a DSP. Accordingly, an individual cannot claim any compensation if an organisation fails to secure its network and information systems (reputation damage, non-compliance penalties and operational costs are often the negative effect of cyber incidents), but logically, cyber incidents only affecting the systems are possibly not infringing any rights either.

NISD obviously refers to security and security measures in many articles, but GDPR also makes some references to the aspect of security, including Art. 28, 30, 33, 35, 40 and 45. GDPR Art. 5 (1) (f) establishes a principle of integrity and confidentiality, including the secure processing of personal data and protection against unauthorised or unlawful processing, destruction or damage. The article stipulates the implementation of appropriate technical or organisational measures as crucial to secure personal data. GDPR Art. 32 stipulates an obligation

[146] GDPR Art. 1, 4 (1). GDPR Art. 2 and 3 establishes the material and territorial scope.

[147] GDPR Art. 4 (2) details the scope of processing. (Markopoulou, Papakonstantinou, & de Hert, 2019). See NISD Art. 16 (5).

[148] GDPR Art. 5 (1) f

for data processors and data controllers to implement security measures, but only to notify security breaches compromising personal data – and not breaches on network and information systems. The article further describes these measures, and stipulates the different factors that controllers and processors have to consider, namely state of the art, costs of implementation, the nature, scope, context and purposes of processing and the risk of infringing the rights of natural persons. Art. 32 (1) a-d further exemplifies measures and capabilities constituting "appropriate", such as encrypting personal data, the ability to ensure confidentiality, integrity, availability and resilience, and to regularly assess the effectiveness of measures. NISD Art. 14 is on the other hand stipulating similar measures to ensure the level of security appropriate to the risk posed, by taking into account state of the art as a guideline to assess if the measures are appropriate, followed by the view to ensure the continuity of essential services. NISD Art. 16 is focusing on five elements which the DSP has to consider. Yet, I would propose that none of the articles are establishing the threshold of "appropriate", even though NIS Cooperation Group Reference Document and Implementing Regulation provides some advice and guidelines. The thesis will return to an assessment on this matter in the next section.

The interviewed cybersecurity leaders have extensive experience in implementing security-related requirements derived from GDPR, and agrees to that the main differences between GDPR and NIS Directive are the purpose and nature of what the two regulations try to protect, and the legal nature of the two regulations. Nonetheless, the legal effect of GDPR being a regulation and not a directive results in a more stringent and harmonised approach, as all countries are bound by the exact same wording. Assessing compliance with GDPR is different, as third parties and self-assessments have a more prominent role than with NISD.[149] Also, although the concept of state of the art itself is not different from NISD, there are in most cases higher expectations for critical sectors to implement strict security measures than for businesses handling personal data. For that reason, it is justifiable that GDPR-related organisations also need to consider other factors, as we do not expect all of them to have state of the art technology. Accordingly, the threshold for critical sectors to implement state of the art measures should be much lower.

[149] GDPR Art. 28 (3) h)

5 The implementation of security requirements

5.1 What is "appropriate and proportionate?"

The previous chapters have elaborated on the legal basis for security requirements, the content of such requirements, and the differentiated legal regime towards the actors that need to adopt measures. Several guidelines and recommendations have been referred to, such as the NIS Cooperation Group Reference Document, ENISA Guidelines on OES Mapping, the Implementing Regulation and more, as both reference points for ensuring convergent implementation among Member States, but also as tools to establish "appropriate and proportionate" measures.

However, neither the Directive nor the Guidelines are specifically stipulating what would constitute an appropriate security level. I would argue that there is no definitive answer as to which measures are "appropriate and proportionate", nor to what standardised threshold constitutes an "appropriate" level of security. The security requirements derived from the Directive is not stipulating an obligation to take certain measures or to prioritise any specific conditions, but they are imposing an obligation to manage the risks related to network and information systems the organisation is using in its operations. Risk management is also needed to prevent incidents from happening, and to minimise their impact when the attack is a fact.

Yet, what constitutes the management of risk?

My definition of risk management is: Knowledge about every relevant factor of a situation becoming a risk, which options that exists to mitigate such risks, and your capability and willingness to either do something about it or tolerate the risk.

Let us provide an example. If an internet virus already is live and out there spreading its malware, and leading to millions of hacked computers; what would your organisation do? Await the situation and hope for not being attacked, or obtain enough information to know which measures are needed to mitigate, execute some preferred measures, continuously assess the situation – and then prepare for the attack? The example provides us the understanding of what risk management and "appropriate and proportionate" actually means. As mentioned above, knowledge is crucial and comprises of two factors: *information* and *competence*. The two factors are dependent on each other, as you need information to obtain knowledge, and you need competence to assess information for the creation of knowledge. And, the reason why technical guidelines, international standards, and recommendations are so important is not because they necessarily provide legal obligations, but because they are the tools the organisation need to obtain information about its own risks – to ultimately manage their risks. Although the term "appropriate and proportionate" measures is not creating a legal threshold, it obliges the organisation to obtain all the knowledge needed to assess whether the level of security is appropriate to the risk posed, and it is therefore relevant to introduce some of the main methodologies and practices that critical sectors have to initiate. DSPs are however subject to a lighter approach, and has a higher degree of freedom than OES, but it is does not mean that the following measures are irrelevant.

5.1.1 Risk management

Risk management is crucial for implementing "appropriate and proportionate" measures, which is supported by 94,1% of the survey recipients as essential (82,3%) or very important (11,7%), and by cybersecurity leaders as the most important action for the purpose of ensuring an appropriate level of security. The response from the survey does not surprise, as risk management is considered the most central parts of the security requirements derived from the Directive.

As DSPs are obliged to take a light approach, the recommendations on risk management for OES does not reflect the minimum measures to ensure an appropriate level of security for DSPs. A "basic" level of risk management for DSPs constitutes security measures such as creating a list of the main risks, their underlying threats, the potential impact of incidents, and making key personnel aware of the main risks.[150]

As OES is posed to a higher risk, they should obtain knowledge systematically, by conducting a regularly updated risk analysis, and identify its Critical Information Systems (CIS).[151] Based on this risk analysis, the OES should create and approve an information system security policy (ISSP) and information security management system (ISMS), and initiate an accreditation process.[152] Compliance is assessed with its ISSP based on a number of indicators related

[150] (European Union Agency For Network And Information Security (ENISA), 2016) 2.4 SO 02 – Risk management. Technical Guidelines connects the available security measures with different sophistication levels, by applying the objectives against recognised international standards, certification schemes and national frameworks.

[151] According to (NIS Cooperation Group, 2018) 14, the risk assessment shall take into account: "new threats, recently discovered weaknesses, loss of effectiveness of measures, changes to the risk situation caused by changes to the system architecture, and any other changes in the risk situation". See NISD Art. 5 (2) b)

[152] According to (NIS Cooperation Group, 2018) footnote 9 on page 14, "'accreditation of CIS' should be understood as the decision by the Operator himself identifying its CIS, the risks associated and the residual risks that the Operator chooses to accept". The CIS accreditation is explained on page 15.

to each CIS, which further results in an information system security audit.[153] Information security risk assessments will determine the risks mentioned in NISD Art. 14 (1), and is critical for the information security risk management process.[154] The main outcome of a risk assessment process is usually an evaluation of the probable risks exposed to a system in light of its context and possible threats.[155]

The organisation can obtain knowledge and increase its competence, adapt organisational measures to systematically assess its risk, and create security awareness among employees, but network and information systems are based on technology – and technical measures are needed to put mitigation into practice. The organisation should obtain knowledge about its assets, by scanning the network for physical and virtual assets, and test the effectiveness and robustness of measures by performing regularly penetration testing. The OES should also configure and segregate systems, perform traffic filtering, and cryptography, which is appropriate and adequate to the risks derived from the risk analysis, aligned with the OES' ISSP, and to ensure the functioning and security of the CIS.[156]

5.1.2 Preventative measures

An essential part of prevention is to detect incidents, which necessitates a security incident detection system, a log system, log correlation and an analysis system.[157] Moreover, the minimisation of impact suggests a procedure for responding to incidents affecting the security, incident reporting, and communication with competent authorities and CSIRTs regarding vulnerabilities, threats and incidents.[158]

5.1.3 The importance of certification

The effectiveness of technical measures are not always the same as what the producer guarantees, and there is an imminent need for certifying the quality of ICT products. The EU has

[153] (European Union Agency for Network and Information Security, 2018, s. 8) defines an information security audit as: "an information systems security audit is an independent review and examination of system records, activities and related documents"

[154] Ibid.

[155] (European Union Agency for Network and Information Security, 2018, s. 10)

[156] See (NIS Cooperation Group, 2018, s. 17 and 18)

[157] Ibid., page 22.

[158] Ibid., page 23.

fortunately in this regard adopted the Cybersecurity Act, which establishes a European cybersecurity certification scheme to ensure an adequate level of cybersecurity ICT products, involving a comprehensive set of technical requirements, standards, rules and procedures established at Union level.[159] The Regulation shall enable a harmonised approach and shall provide mechanisms to establish certification schemes to attest that products, services and processes have been evaluated in compliance with security requirements.[160] The most important part of the Regulation is the inclusion of security objectives which shapes the design of the European cybersecurity certification scheme, including protecting data against unauthorised access and destruction, identity access management, vulnerability management, log monitoring and retention, and security by default and design[161]. Potentially, I would presume that if the Regulation succeeds in achieving its ambition, it can be a game changer for securing network and information systems. The fact that the certification framework is adopted as a Regulation could impact the level of security in the EU significantly, as OES and DSPs are dependent on knowledge about whether ICT services and products work as intended.

5.1.4 The role of voluntary standards

According to the survey, security professionals consider the role of voluntary standards as very important (47%) and essential (17,6%) to help implementing security requirements. However, 35% think this is moderately important, which also is a quite high number. Not all standards are important, and in some cases voluntary standards are designed as vague criteria which is easy to comply with. Such scenarios could weaken the regime of international recognised standards. I would probably have a more detailed understanding of this issue if there was some follow-up questions on the role of international standards.

Member States shall encourage OES and DSP to use relevant European or internationally accepted standards and specifications in order to promote "convergent implementation of Article 14 (1) and (2) and Article 16 (1) and (2)", and not impose an obligation to use a specific type of technology.[162] ENISA, shall detail advices and guidelines related to technical field of security requirements for OES and DSP, and shall also cooperate with the NIS Cooperation

[159] Cybersecurity Act, Art. 1 (1) b and 2 (9) (European Commission, 2019)

[160] Ibid., Art. 46 (1) and (2)

[161] Ibid., Art. 51, 51 a), b), c), d), e), i)

[162] NISD Art. 19 (1)

Group, and assist the Union institutions and Member States in implementing necessary policies to satisfy the legal requirements for securing network and information systems[163].

In case of the main differences between an industry standard, such as ISO27001, and the NIS Directive, the cybersecurity leaders underline that although the former is non-binding and the latter is legally binding, the relationship between norms and legislation is tightly integrated. Norms play a pivotal role in interpreting discretionary legal obligations into concrete security controls. The voluntary standards also differs in nature and scope, and there are many sector-specific standards which the organisation can apply. They are also frequently updated, recognised by the industry, and impose requirements that can help the organisation to achieve an appropriate level of security. The security leaders elaborate that the preferred method of risk management is to map its requirements with other relevant voluntary standards, and then perform risk assessments to find appropriate controls. Thus, complying with for example ISO27001 makes it a lot easier for an organisation to also comply with NISD.

5.1.5 The role of "state of the art"?

Both implementation of risk-based security requirements imposed on OES and DSP has to take into account the "state of the art". The Task Force "State of the art", launched by The IT Security Association Germany (TeleTrusT), stipulated recommendations and guidelines for evaluating technical and organisational measures in light of state of the art.[164] The report was originally made for determining this terminology within the meaning of the German IT Security Act (ITSiG) and the GDPR, but can also serve as a reference for contractual agreements, classification of security measures implemented, and procurement processes.[165] Thus, the guidelines will be applicable for the implementation of security requirements derived from the NISD.

The guidelines are referring to the Kalkar decision as the innovator of the "three-step theory", meaning state of the art is positioned between the more established "generally accepted rules of technology" and the more innovative "existing scientific knowledge and research", in which the latter has low general recognition and been least proven in practice.[166]

[163] NISD Art. 19 (2) and Cybersecurity Act (European Commission, 2019) Art. 5 (2), cf. NISD Recital 38

[164] Both NISD Art. 14 (1) and 16 (1) state that measures ensuring level of security appropriate to the risk, shall have regard to the "state of the art". (IT Security Association Germany (TeleTrusT) and ENISA, 2019, s. 6)

[165] Ibid.

[166] (Kalkar Case I (1978), 1978)

State of the art can be described as: “a subject’s best performance available on the market to achieve an object. The subject is the IT security measure; the object is the statutory IT security objective”. [167]

The individual states of technology starts with a measure originating (stage of “existing scientific knowledge and research”), then introduced on the market (“state of the art” stage), and then distributed and recognised on the market to an extent eventually leading to the stage of “generally accepted rules of technology”. [168] To prove that an organisation has implemented security measures within the stage of “state of the art”, the organisation has to compare the alternatives available on the market regularly and transparently.[169] Specifically, an implementation of state-of-the-art risk management requires the organisation to analyse, assess and handle weak points, values, effects and threats, take control over residual risk by senior management and continually optimise the overall risk exposure.[170]

The cybersecurity leaders underline the importance to apply “state of the art” in the combination of what is “appropriate” and “proportionate” for the organisation, meaning that the need for procuring the best available products and services should be assessed regularly in light of the management of risks – as risks may increase and products will improve over time.

5.1.6 Considerations

The analysis of security requirements proposes that the threshold is higher for implementing “appropriate and proportionate” measures for OES, than for DSPs. However, establishing an “appropriate” security level within the organisation depends on obtaining knowledge about all relevant factors of the risk and options that exists to mitigate, and having the capabilities and willingness to either do something about it or accept the risk. Risk management should be based on a combination of complying with regulations and international recognised standards, and state of the art should be taken into account in the establishment of an “appropriate” level of security. Risk posed to security of network and information systems will have sector-specific variations, geographical variations, and depend on the criticality of the sector and the nature of the specific business. However, having the capabilities and willingness suggests competent internal resources. The industry of information security lacks of competence, and one can argue in this matter that the rise of new academic specialisations, such as Master’s degree in Cybersecurity, and certifications, such as CISA, CISSP, and CCSK, is a response to this trend. As we

[167] (IT Security Association Germany (TeleTrusT) and ENISA, 2019, s. 11)

[168] (IT Security Association Germany (TeleTrusT) and ENISA, 2019, s. 12)

[169] Ibid.

[170] (IT Security Association Germany (TeleTrusT) and ENISA, 2019, s. 63)

have seen previously in this thesis, many Member States relies on the OES to self-assess parts of the identification process, and even parts of the information security audits. Thus, maintaining and enhancing the internal competence is vital to ensure that knowledge is obtained. Additionally, the adoption of the Cybersecurity Act may impact the security level in the EU significantly, as OES and DSPs can trust whether ICT products and services function as they intend to do, which would gain knowledge of what measures are proportionate to achieve an appropriate level of security.

5.2 Comparing the implementation of security requirements in Member States

The Member States shall adopt and publish the laws, regulations and provisions necessary to comply with the Directive by 9 May 2018, and apply measures from 10 May 2018.[171] The EU Commission has the responsibility to assist Member States in implementing EU laws correctly, and take steps if an EU country does not fully incorporate a directive or fails to apply the EU law.[172] The Commission may initiate an infringement procedure if an EU country fails to implement EU law[173], and penalties can be initiated, cf. NISD Art. 21. Member States stipulates rules on penalties in cases of violations of national provisions, which should be *"effective, proportionate and dissuasive"* .[174]

5.2.1 Three dimensions of implementation in EU countries

The NIS Directive is transposed in all 28 EU countries, and the implementation of security requirements in EU countries can be divided into three dimensions: the wording of the regulation, the organisation of requirements, and the usage of common vs specialised security requirements.[175]

I will take a further look at the three dimensions.

[171] NISD Art. 25 (1)

[172] TFEU Art. 288

[173] TFEU Art. 258

[174] NISD Art. 21

[175] However, 17 EU countries did not meet the deadline (9 May 2018), and the EU Commission sent a formal letter of notice. Belgium and Luxembourg were the last two countries failing to implement the Directive, and received a reasoned opinion from the EU Commission, with the threat of the Court of Justice intervening if not complying within two months.

5.2.1.1 Wording of the transposed national legislation

The research of national transpositions in Ireland, Luxembourg, Malta, the Netherlands, Portugal, Spain, Sweden and the UK suggests that the security requirements in national legislation is codified similarly or almost identically as in the NIS Directive.

In Belgium, security requirements are transposed into the adoption of the Act establishing a framework for the security of network and information systems of general interest for public security, Art. 20 and Art. 33. [176] The wording in these two articles are identical as the NISD Art. 14 and 16. The competent authority is responsible for monitoring and coordination the implementation of the law, cf. Art. 7.

The research of national transpositions in Estonia, Greece, France, Latvia, Poland and Slovenia suggests that the security requirements in national legislation is more detailed than in the NIS Directive.

In Estonia, security requirements are transposed into the adoption of the Cyber Security Act, and its §7 stipulates the service provider (OES) to apply security measures to prevent and resolve a cyber incident, as well as mitigating the effects, by taking actions, such as performing a system risk analysis, monitoring the systems, and verify the adequacy of security measures[177]. Digital service providers are obliged to take appropriate and proportionate measures which is stipulated in §10. The paragraph makes references to the Implementing Regulation and applies the same language as NISD.

5.2.1.2 Organisation of obligations

In Austria, security requirements are transposed into the adoption of Network and Information Systems Security Act §17 (OES), §21 (DSP) and §22 (public administration bodies). [178] The wording in all three paragraphs are almost identical with NISD Art. 14 and 16, but merges the obligations in 14 (1) / 16 (1) and 14 (2) / 16 (2) into one obligation, namely to take appropriate and proportionate technical and organisational measures relating to network and information systems which they use to provide their service, and must take into account state of the art, and appropriate to the risk. The factors DSPs have to consider are identical with Art. 16 (1). The Federal Minister of Interior has the task to verify the security requirements, cf. §5.

[176] (FEDERALE OVERHEIDSDIENST KANSELARIJ VAN DE EERSTE MINISTER (FEDERAL PUBLIC DEPARTMENT OF THE FIRST MINISTER), 2019)

[177] (Riigikogu (Estonian Parliament), 2018) §7 (1), §7 (2) 1 and 2, §7 (2) 3, §7 (2) 5

[178] (Der Nationalrat (The National Council), 2018)

5.2.1.3 The usage of common vs specialised security requirements

The research of national transpositions in Denmark, Finland, Germany and Hungary illustrates that the common security requirements are delegated into sectorial focused (lex specialis) security requirements.

In Denmark, security requirements are transposed into the adoption of 12 new sectorial focused bills, such as the health sector, transport, water distribution, oil sector, financial market infrastructures etc. The wording of the security requirements are identical across the different segments.

5.3 The case of Norway: comparing NISD with Sikkerhetsloven

The NIS Directive is not yet transposed into Norwegian legislation, as it is not formally part of the EEA Agreement. However, the Directive is EEA relevant and there is no cross-sectorial or sector-specific laws in Norway providing equivalent requirements to the Directive.[179] The Directive has similarities with the Norwegian Security Act (Sikkerhetsloven), but the two legislations' purposes and mechanisms are different.[180] The identification of actors are fundamentally different, the requirements are different, but the result is similar: applying risk management to implement appropriate measures and mitigate the impact of incidents. The Justice Department is currently working on the implementation of the NIS Directive into Norwegian legislation, and has been specifically discussing the consistency of methodological approaches. The representatives are aware of the inconsistencies practiced among Member States, and are focusing on ensuring harmonisation to the greatest extent possible. The NIS Directive has been out on public review since early 2019, and the Department is planning to implement the Directive by 2020 no matter how much time the process of including the legislation into the EEA Agreement will take. The Department considers "appropriate" as a minimum level of security, although the means of getting there implies a thorough assessment. The basic principles of National Security Agency (NSM) provides guidance on the assessment of appropriate level of security, which is based on recognised international standards and frameworks.

[179] (Justis- og Beredskapsdepartementet, 2018, s. 6)

[180] (Brækhus Advokatfirma DA)

5.4 Achieving a “high common level”?

The main purpose of the Directive needs to be interpreted in the light of the main obligations and capabilities of the Directive, described in Art. 1 (2). Thus, security requirements imposed on OES and DSP cannot fulfil the purpose of the Directive alone, but will play a vital role together with the adoption of national cybersecurity strategies providing frameworks for the Member States, participation in the NIS Cooperation Group and CSIRTs network to promote a consistent implementation and improve the incident response capabilities, establishing national competent authorities to enforce compliance, and creation of single point of contact to safeguard swift notification of incidents. Hence, achieving the purpose of a “high common level of security” depend on far more factors than solely the security requirements imposed on OES and DSP. However, it is relevant to interpret whether the implementation of security requirements is aligned with the purpose of the Directive, and assess whether there is potential for improvement.

From the perspective of security requirements, the next section will assess whether the Directive is capable of achieving a *common* level, followed by the capability of achieving a *higher* level.

The identification of essential services is the primary step in imposing *common* security requirements consistently towards a set of actors. The EU report on methodological inconsistencies shows a trend of fragmented approaches all over the Union. Supposedly, as one of the main purposes is a *common* level of security, the lack of consistency illustrates that the Directive is not well-designed to achieve this purpose. Member States are also not willing or capable of identifying essential sectors consistently or consult each other in the process.

The implementation of *common* security requirements requires *common* obligations for OES and DSPs. However, although the two categories are obliged to comply with significantly different obligations, as the Directive does differentiate intentionally, it would seem logical that the legislation is referring to *a common level* within the categories. Moreover, there are also issues arising with this view, as sector-specific rules can impose equivalent or stricter obligations on certain sectors, and as the individual assessment related to risk management can create substantial differences on the implementation of security measures in organisations within the same sector. Whether the law-makers are intentionally referring to *common* as a level which is similar across the Union, or as a *common minimum* level remains unclear. However, it seems more logical that the Directive provides a *common framework* by imposing obligations to manage risks to ensure an appropriate level of security.

This also aligns with the cybersecurity leaders' view, as they do not consider the potential level to be common, due to the differentiation between OES and DSP, between OES-sectors and between countries.

When it comes to creating a *higher* level of security, the rationale provided previously in this thesis suggests that most of the sectors did not have security requirements to comply with, and the level of preparedness among Member States were uneven across the Union. By referring the Directive to frequently updated and recognised international standards, such as ISO27001, and introducing a culture of risk management on the agenda for critical sectors, the purpose of a *higher* level of security is definitely easier to satisfy, at least on the minimum level. In this regard, the security leaders are positive about the Directive possibly leading to a higher level of security, as it requires organisations to take into account security of network and information systems. They further elaborate that the minimum level will possibly be strengthened by the Directive, as it requires organisations within critical sectors to consider security. However, organisations already investing heavily in security would be less affected by the security requirements, as they have most capabilities in place to comply with the Directive. The survey illustrates that 94% of the security professionals consider it likely (76%) or very likely (18%) that the Directive will result in a higher common level of security of network and information systems in the EU. This trend is positive for the industry, and something to take into account for the further implementation of the Directive.

5.5 Judicial policy considerations

Evidence from cybersecurity standards within critical infrastructure illustrates that risks are difficult to measure, predict and regulate, as complex systems and uncertainties leads to highly consequential and rare events, raising the question whether regulatory efforts or self-regulation is the most appropriate action.[181] Adoption of legislations takes often several years, and at the same time state of the art technology and the range of security controls has changed significantly, making the regulations outdated before they have entered into force. Moreover, this situation creates a dilemma: a higher degree of detailed requirements would help the security legislation to become more transparent and predictable for organisations to comply with, but also create a legislation that quickly becomes totally outdated. Adopting general and discretionary wording for the common requirements, and impose specialised requirements where it is appropriate could avoid a regulation losing its momentum even before it has been implemented

[181] (Clark-Ginsberg & Slayton, 2018, s. 340)

in EU countries. It is important to take notice in this regard that the process of creating the NIS Directive started in 2013, and it is now 7 years since the first proposal was written. In cybersecurity, everything can change in such an amount of years. Thus, by providing a common minimum level and dynamical requirements that can change frequently, the NIS Directive can last longer and remain relevant.

The cybersecurity leaders and the survey both agree that the attention for the NIS Directive has been little, especially compared to the GDPR. Organisations asking about security requirements do not necessarily have inquiries specifically about the Directive, or are motivated to comply with certain requirements, but could indirectly be subject to requirements that derives from the Directive – even though this is not communicated explicitly. However, the two groups of organisations that are often asking for the NIS Directive security requirements are either organisations within a critical sector (the company is an OES and have been subject to strict security requirements for many years), or have already invested heavily in a high security posture. Comparing attention with the GDPR would probably be unfair, as the Regulation is both protecting fundamental rights for individuals and imposing duties on organisations to protect personal data. However, pushing security of network and information systems higher up on the political agenda would also probably create security awareness, which is an important part of sound cybersecurity practice.

Increasing the level of security would result in investments which from an economic perspective cannot be returned – as the business lack incentives for the implementation of appropriate security measures.[182] The burden on companies for implementing security measures is addressed in the Directive, and requires organisations to evaluate whether the measures are "proportionate". Disproportionate burdens on organisations can have negative effects, such as weakening the support for the Directive, and leading to financial loss for organisations. The constant pressure on compliance, and check-box-solutions is only confusing the potential customers to procure something that has not been proven to provide an appropriate level of security. The cybersecurity leaders interviewed in this thesis have mentioned this trend as problematic, as the market is full of products and services, and a lack of skilled talent. The combination often results in organisations implementing disproportionate measures, as they do not have the competence to assess whether a measure is needed or not. The new EU certification regulation

[182] (European Commission, 2013) 4.1.5.2

will hopefully provide a more uniform certifying scheme across the Union. The cybersecurity leaders argue that the Directive entails a proportionate burden for most organisations, but that small and non-critical DSPs should assess whether to implement measures or not. The implementation of GDPR also reminds us of how the massive attention for compliance can create panic among organisations, leading to a disproportionate high investment in measures. As the NIS Directive also imposes requirements on data-related activities, organisations could react by acting reluctant to yet another regulation. The cybersecurity leaders refer to this trend as a possible explanation for the lower attention paid to the Directive.

6 Conclusion

The thesis has provided some important findings on the value of consistency when identifying actors that are subject to the Directive. Experiences show that EU countries differ significantly on how they define essential services, what kind and the levels of thresholds that need to be satisfied, which authorities that are mandated to identify, and whether to perform assessments on dependency to network and information systems or not. One could think that the implementation efforts by the Member States solely explains the trend, but the real issue is the design of the Directive. Simply put, an EU directive entails an instruction that each Member State has to follow when making national legislation.[183] If the instruction does not provide any obligations to follow a consistent methodology to identify OES, the Member States are permitted to do what is best for them, and not necessarily what is best for the Union. Conversely, if the instruction stipulated a clear framework with binding rules on methodological approaches, the EU countries would have to comply. Thus, the EU rules on identification of OES are working as they are intended to.

Security requirements derived from NISD follow much of the same wording as other EU regulations, such as GDPR, on taking “appropriate and proportionate” organisational and technical measures. However, the legal obligation of these requirements is not to stipulate that certain security controls have to be implemented, but to find the organisation’s appropriate level of security. Discovering such level is based on a thorough, continuous and systemic risk management process, including legal, technical and organisational perspectives on multiple levels within the organisation. I would argue that there is no definitive answer as to what constitutes “appropriate” and “proportionate” as no organisations have the exact same risks, vulnerabilities

[183] (European Parliament Information Office Finland, Helsinki, 2014)

and assets. The only way organisations' can achieve this level of security is to obtain as much knowledge as possible, combined by receiving all relevant information about the business and its risks and having the skilled competence to apply the information, to assess which measures that have to be implemented. Managing risks also requires information security audits, which enforces the compliance. National competent authorities and qualified third party auditors play important roles in maintaining this compliance, and on this matter, only OES are audited regularly – while DSPs are self-assessing their management of risks.

The Directive is created as a flexible instrument providing harmonised rules on a minimum level, which has both proven to be positive for Member States, as they have varying challenges and priorities, but also negative for the convergent implementation of the Directive. Dynamic requirements are necessary, as the technical development keeps a significant higher pace than the legislation process, and effective, as the obligation of performing risk management produces unique measures appropriate to the specific organisation – not measures that are proportionate for some and disproportionate for others. However, organisations can assess their risks and vulnerabilities, but they are dependent on a comprehensive guidance to find the appropriate security controls. ENISA and NIS Cooperation Group provides detailed technical guidelines on these matters, but international standards has a much more prominent role, as they are frequently updated and well recognised by the industry. Sector-specific standards provide a systematic approach to risk management, and make the road a lot easier for critical sectors to ensure an appropriate level of security, as security objectives are broken down into categories and security controls. However, standards are a market-driven response to compliance, which provide some downsides, such as an influx of new standards with new requirements and controls provided in an ecosystem of compliance services where all the providers have a financial benefit of upgrading the technology constantly. For that reason, the recently adopted EU Cybersecurity Certification Framework could be a valuable instrument, as it does not have the same financial incentives, which could provide an option with a higher degree of neutrality. Succeeding with this framework depends on several factors, including a balance between the degree of detail and costs in the certification requirements, as more stringent requirements imposes higher costs for the organisation. The requirements also need to be as proportionate as possible, meaning that they should focus on what actually creates a higher level of security in practice, and avoid unnecessary and disproportionate requirements. Furthermore, a product or service adequate for today's threat landscape is not adequate for tomorrow's threat landscape, meaning that requirements should change regularly – to ensure an effective regime. A good example is the case of CE mark certification testing, which the public authorities assesses regularly. However, security flaws were discovered by a private company, leading to the public authority initiating new tests discovering that certain smart watches did not satisfy the requirements.[184] The public authority had the responsibility to perform audits, but were not able to conduct them on a satisfactory level. Thus, the mechanisms for compliance has to work in practice.

Security requirements cannot alone achieve a high common level of security of network and information systems in the EU, as this ambition depends on several other factors, such as the national cybersecurity capabilities, the cooperation at EU level, and the national implementation effort. Achieving a “high and common” level of security does also not necessarily mean all critical sectors having the same high and common level, but that the minimum level is increased through common requirements. Such common requirements could differ between sectors and categories, which makes them even less common. However, it is still early to predict if the security level will be impacted by the Directive, and the experiences in the coming years will prove whether the ambition has been achieved or not. An interesting further research on the topic would be to study if Member States implement and define more consistently by themselves or if the EU has to create binding rules, rather than recommendations, to mitigate the inconsistencies that exists today. Furthermore, another interesting study would be to assess whether penalties will be used by the Court of Justice, other EU institutions, or by national authorities, towards Member States, OES or DSPs for non-compliance with the Directive. As we have experienced with the GDPR, risk of reputation damage and high fines affecting the organisation financially can create a panic to suddenly take measures, not necessarily proportionate, to be on the safe side.

The thesis has based its findings on a doctrinal legal and technical research, and the conduction of three in-depth interviews and a survey. Interpreting only the legal source establishing the security requirements is insufficient to assess whether the Directive is designed to achieve its purpose, as cybersecurity is a multidisciplinary field, meaning that one needs both legal, organisational and technical capabilities to be able to perform satisfactory risk management and ensure an appropriate level of security. The non-existent case law makes it more dif-

[184] (Nasjonal kommunikasjonsmyndighet, 2018)

ficult to evaluate whether the Directive functions properly, or if has flaws that needs to be altered, and it would definitely be valuable to have more court cases as a legal basis. A possible further research topic could also be to explore the notification requirements alongside the research on security requirements, as there are overlaps in how to manage the risks and how to respond to incidents. Finally, the suggestions to further research and the questions that arises through this thesis implies that the relationship between legally binding norms and cybersecurity is an emerging field, and it needs to be assessed holistically and multidisciplinary in light of a rapid technological development.

7 Bibliography

African Union. (2014). *The African Union's Convention on Cyber Security and Personal Data Protection.* Malabo: African Union.

Baratta, R. (2014). *19th Quality of Legislation Seminar: "EU Legislative Drafting: Views from those applying EU law in the Member States".* Brusssels: European Commission.

Brækhus Advokatfirma DA. (u.d.). *Brækhus Advokatfirma.* Hentet fra IKT-sikkerhetsutvalgets utredning og forslag om gjennomføring av NIS-direktivet er sendt på høring: https://braekhus.no/ikt-sikkerhetsutvalgets-utredning-og-forslag-om-gjennomforing-av-nis-direktivet-er-sendt-pa-horing/

China Cyber Security Coordination Bureau. (2017). *Regulations on the Security Protection of Critical Information Infrastructure (Consultation Draft).* Beijing: China Cyber Security Coordination Bureau.

Clark-Ginsberg, A., & Slayton, R. (2018). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, 339-346.

Cloud Security Alliance. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0.* Seattle, WA: Cloud Security Alliance.

(1950). *Convention for the Protection of Human Rights and Fundamental Freedoms.* Rome: European Court of Human Rights, Council of Europe.

Council of Europe. (2001). *Convention on Cybercrime.* Budapest: Council of Europe.

Council of Europe. (2001). *Explanatory Report to the Convention on Cybercrime.* Budapest: Council of Europe.

Council of Europe. (2020, 01 28). *Council of Europe*. Hentet fra Internet Freedom: https://rm.coe.int/leaflet-internet-freedom-en-/16808b53dd

Crumpler, W., & Lewis, J. (2019). *The Cybersecurity Workforce Gap*. Center for Strategic & International Studies.

Der Nationalrat (The National Council). (2018). *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Federal law to ensure a high level of security for network and information systems).* Vienna: Der Nationalrat (The National Council).

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010. (2015). *Official Journal of the European Union*, 35-127.

Direktoratet for samfunnssikkerhet og beredskap (DSB). (2019). *Analyser av krisescenarioer 2019.* Oslo: Direktoratet for samfunnssikkerhet og beredskap (DSB).

ESI ThoughtLab. (2019). *The Cybersecurity Imperative Pulse Report.* Philadelphia, PA: ESI ThoughtLab.

EU Commission. (2019, July 15). *European Commission | Digital Single Market*. Hentet fra Policy: The Directive on security of network and information systems (NIS Directive): https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Commission. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*, 31-50.

European Commission. (2002). Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). *Official Journal of the European Union,* 33-50.

European Commission. (2003). COMMISSION RECOMMENDATION of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. *Official Journal of the European Union*.

European Commission. (2008). Consolidated version of the Treaty on the Functioning of the European Union - PROTOCOLS - Protocol (No 2) on the application of the principles of subsidiarity and proportionality. *Official Journal of the European Union*, 206-209.

European Commission. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union,* 75-82.

European Commission. (2011, January 21). *European Union*. Hentet fra Emissions Trading: Q & As following the suspension of transactions in national ETS registries for at least one week from 19:00 CET on Wednesday 19 January 2011: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_11_34

European Commission. (2013). *COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union.* Brussels: EU Commission.

European Commission. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*, 73-114.

European Commission. (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. *Official Journal of the European Union*, 1-15.

European Commission. (2016). Regulation (EU) 2016/679 of the European Parliament and of 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. *Official Journal of the European Union,* 1-88.

European Commission. (2017). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148.* Brussels: European Commission.

European Commission. (2018). COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of NIS Directive as regards further specification of the elements to be taken into account by digital service providers. *Official Journal of the European Union*.

European Commission. (2018, 07 11). *EUR-LEX.* Hentet fra European Union directives: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14527&from=EN

European Commission. (2018, July 19). *European Commission | Digital Single Market.* Hentet fra Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity: https://ec.europa.eu/digital-single-market/en/news/commission-asks-member-states-transpose-national-laws-eu-wide-legislation-cybersecurity

European Commission. (2019). REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Cybersecurity Act. *Official Journal of the European Union*.

European Commission. (2019). *REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU.* Brussels: European Commission.

European Cyber Security Organisation & DigitalEurope. (2019, March 25). *DigitalEurope*. Hentet fra NIS Implementation Tracker: https://www.digitaleurope.org/resources/nis-implementation-tracker/

European Parliament Information Office Finland, Helsinki. (2014). *Information campaign of the European Parliament.* Hentet fra How the European Union works: https://europarlamentti.info/en/European-union/how-the-EU-works/

European Union. (2012). *Treaty on the Functioning of the European Union.* Brussels: European Union.

European Union Agency For Network And Information Security (ENISA). (2016). *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers.* Heraklion: European Union Agency For Network And Information Security (ENISA).

European Union Agency for Network and Information Security (ENISA). (2017). *Incident notification for DSPs in the context of the NIS Directive.* Heraklion: European Union Agency for Network and Information Security (ENISA).

European Union Agency For Network and Information Security (ENISA). (2017). *Mapping of OES Security Requirements to Specific Sectors.* Heraklion: European Union Agency For Network and Information Security (ENISA).

European Union Agency for Network and Information Security. (2018). *Guidelines on assessing DSP and OES compliance to the NISD security requirements Information: Security Audit and Self – Assessment/ Management Frameworks.* Heraklion: European Union Agency for Network and Information Security.

Evans, M. D. (2014). *International Law.* Oxford: Oxford University Press.

FEDERALE OVERHEIDSDIENST KANSELARIJ VAN DE EERSTE MINISTER (FEDERAL PUBLIC DEPARTMENT OF THE FIRST MINISTER). (2019). *7 APRIL 2019. - Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de (Law establishing a framework for the security of network and information systems of general interest for public security.* Brussels: FEDERALE OVERHEIDSDIENST KANSELARIJ VAN DE EERSTE MINISTER (FEDERAL PUBLIC DEPARTMENT OF THE FIRST MINISTER).

Fidler, D. P. (2015). Whither the Web: International Law, Cybersecurity, and Critical Infrastructure Protection. *Georgetown Journal of International Affairs,* 8-20.

Finnish Transport and Communications Agency - National Cyber Security Centre. (2020, 01 14). *NCSC - FI.* Hentet fra Subjects to regulation:

https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/subjects-regulation

Georgieva, L. (2016). The First EU-Wide Legislation on Cybersecurity. *European Energy Journal*, 62-76.

Haber, E., & Zarsky, T. (2017). Cybersecurity for Infrastructure: A Critical Analysis. *Florida State University Law Review*, ss. 516-576.

International Law Commission. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts. *Yearbook of the International Law Commission*, 31-143.

Ireland National Cyber Security Centre. (2019). *NCSC*. Hentet fra Digital Service Providers: https://www.ncsc.gov.ie/dsp/

IT Security Association Germany (TeleTrusT) and ENISA. (2019). *Guideline "State of the Art": Technical and organisational measures.* Berlin: IT Security Association Germany (TeleTrusT) .

Judgment of the Court (Fifth Chamber) of 19 November 1998. - Criminal proceedings against Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn, C-162/97 (Fifth Chamber, Court of Justice November 19, 1998).

Justis- og Beredskapsdepartementet. (2018). *Høringsnotat: Høring om utkast til lov som gjennomfører NIS-Direktivet i norsk rett.* Oslo: Justis- og Beredskapsdepartementet.

Justis- og beredskapsdepartementet. (2018). *Lov om nasjonal sikkerhet (sikkerhetsloven).* Oslo: Justis- og beredskapsdepartementet.

Kalkar Case I (1978), 49 BVerfGE 89 (Federal Constitutional Court August 8, 1978).

Mačák, K. (2016). Is the International Law of Cyber Security in Crisis? . *2016 8th International Conference on Cyber Conflict*, 127-139.

Markopoulou, D., Papakonstantinou, V., & 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: The International Journal of Technology Law and Practice*.

Merriam-Webster. (2019, January 10). *Merriam-Webster*. Hentet fra Legal Person Legal Definition | Merriam-Webster Law Dictionary: https://www.merriam-webster.com/legal/legal%20person

Merriam-Webster. (2019, January 10). *Merriam-Webster*. Hentet fra Gap | Definition of Gap by Merriam-Webster: https://www.merriam-webster.com/dictionary/gap

Nasjonal kommunikasjonsmyndighet. (2018, January 16). *Nasjonal kommunikasjonsmyndighet (Norwegian).* Hentet fra Nkom: for dårlig kvalitetssikring ved omsetning av smartklokker for barn: https://www.nkom.no/aktuelt/nyheter/nkom-for-d%C3%A5rlig-kvalitetssikring-ved-omsetning-av-smartklokker-for-barn

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An Introduction to Information Security.* Gaithersburg, MD: National Institute of Standards and Technology.

NIS Cooperation Group. (2018). *Identification of Operators of Essential Services: Reference document on modalities of the consultation process in cases with cross-border impact.* Brussels: European Commission.

NIS Cooperation Group. (2018). *Reference document on security measures for Operators of Essential Services.* Brussels: European Commission.

North Sea Continental Shelf, 327 (International Court of Justice February 20, 1969).

OPINION OF THE EUROPEAN CENTRAL BANK of 25 July 2014 on a proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. (2014). *Official Journal of the European Union*, 4-11.

Porcedda, M. G. (2018). Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer L aw and Security Review,*, 1077-1098.

Riigikogu (Estonian Parliament). (2018). *Küberturvalisuse seadus (Cyber Security Act).* Tallinn: Riigikogu (Estonian Parliament).

S.S. Lotus (France v. Turkey), Series A - No. 10 (Permanent Court of International Justice September 7, 1927).

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health. - Reference for a preliminary ruling: Corte suprema di Cassazione - Italy. - Obligation to request a preliminary ruling, 283/81 (Corte suprema di Cassazione (Supreme Court of Cassation) October 6, 1982).

Tabrizi, B., Lam, E., Girard, K., & Irvin, V. (2019, March 13). *Harvard Business Review.* Hentet fra Change Management: Digital Transformation Is Not About Technology: https://hbr.org/2019/03/digital-transformation-is-not-about-technology

The Norwegian Board of Technology. (2017). *This Time It's Personal: The Digital Shift in The Public Sector.* Oslo: The Norwegian Board of Technology.

U.S. Congress. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.* Washington D.C.: U.S. Congress.

Vaquero, N. (2013). Five Models of Legal Science. *Revus*, 53-81.

8 Annex I – Interview questions

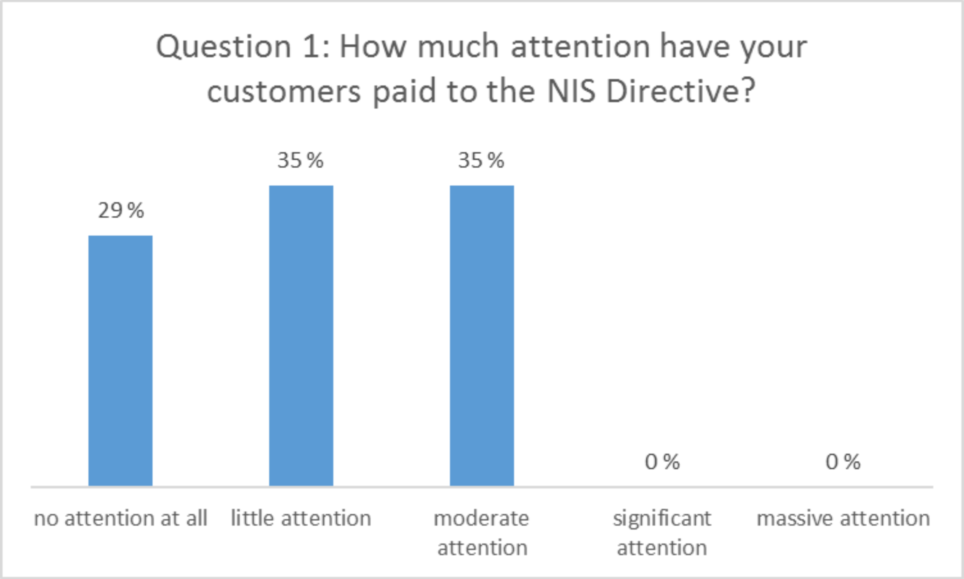
1. What is your experience in the implementation of security requirements derived from the NIS Directive? Is the Directive a topic among your customers?
2. Classifying an organisation as operator of essential services requires three cumulative criteria to be satisfied. Typical examples are provided in NISD Annex II. However, several EU countries have added other sectors, and applied different methodologies. What do you think about the identification of OES, the criteria, and the inconsistency in the EU?
3. Are the security requirements in GDPR (i.e. Art. 32) a topic among your customers, and if yes – what kind of measures do you think are relevant for ensuring compliance?
4. What do you think are the main differences and commonalities between GDPR and NIS Directive?
5. NIS Directive Art. 14 and 16 stipulates operators of essential services and digital service providers to take appropriate and proportionate security measures. What do you think is required to comply with the security requirements in NIS Directive (Art. 14 and 16)? Do you think the wording of the requirements should be more detailed, and should the requirements be specialised for each sector or common for many sectors? Which role should the authorities take to ensure and enforce compliance?
6. What do you think are the main steps in the process of implementing security requirements in organisations?
7. How important do you think technical measures, such as IT security architecture and identity and access management, are for securing network and information systems?
8. State of the art can be described as: *"a subject's best performance available on the market to achieve an object. The subject is the IT security measure; the object is the statutory IT security objective".* What do you think constitutes the threshold of "state of the art" technology?

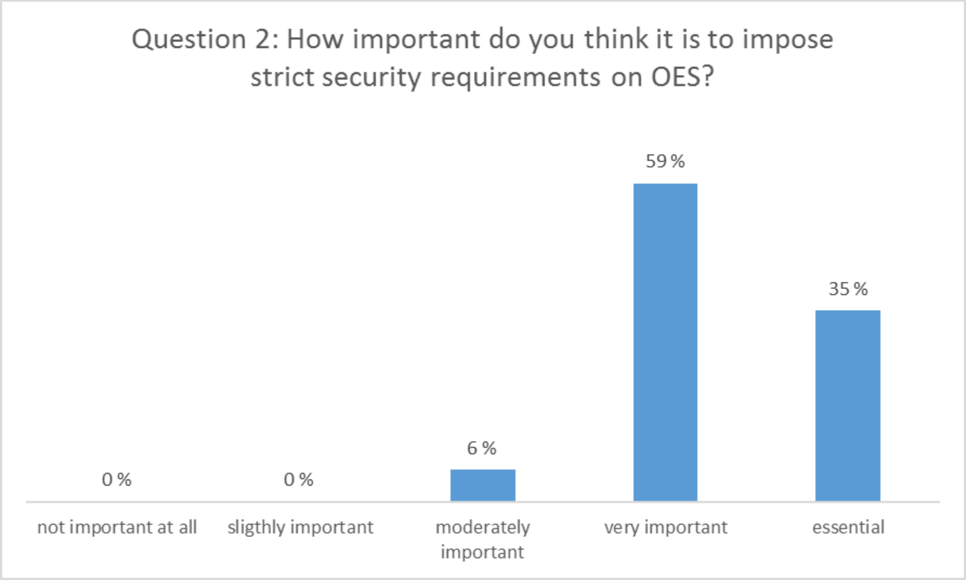
   What do you think are the main differences and commonalities between non-binding industry standards, such as ISO27001 and NIST Cybersecurity Framework, and legislation, such as GDPR and NIS Directive? Which role do you think voluntary norms and standards play for the interpretation of cybersecurity legislation?
9. To what extent you think the implementation of the Directive in the EU could lead to a higher common level of security of network and information systems?

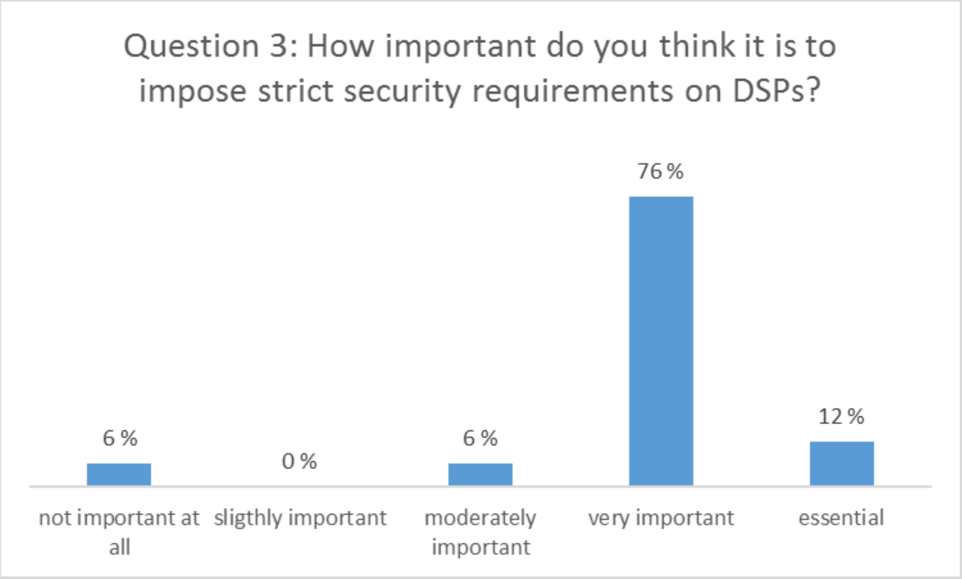
10. To what extent you think the implementation of the Directive in the EU could lead to a disproportionate burden on companies?

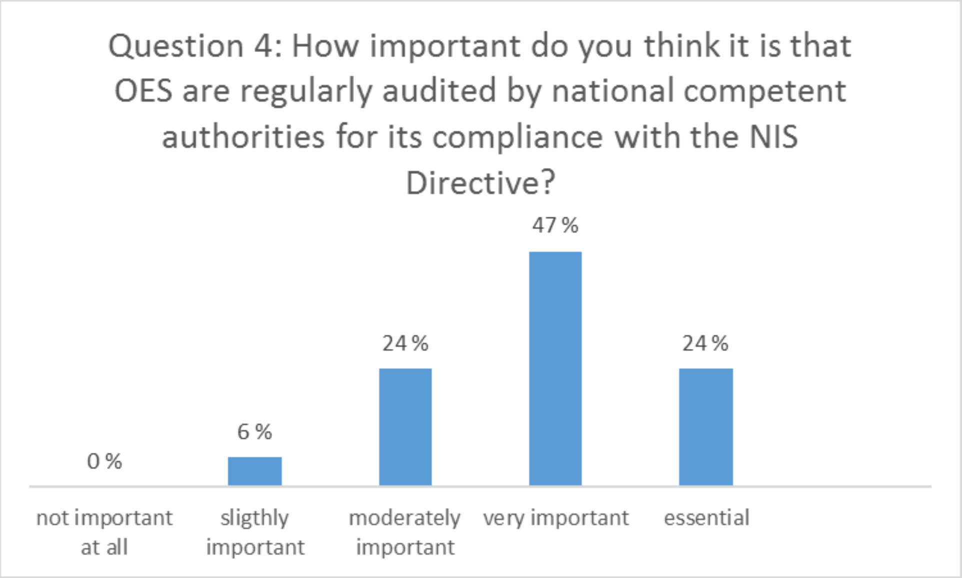
9 Annex II – Survey

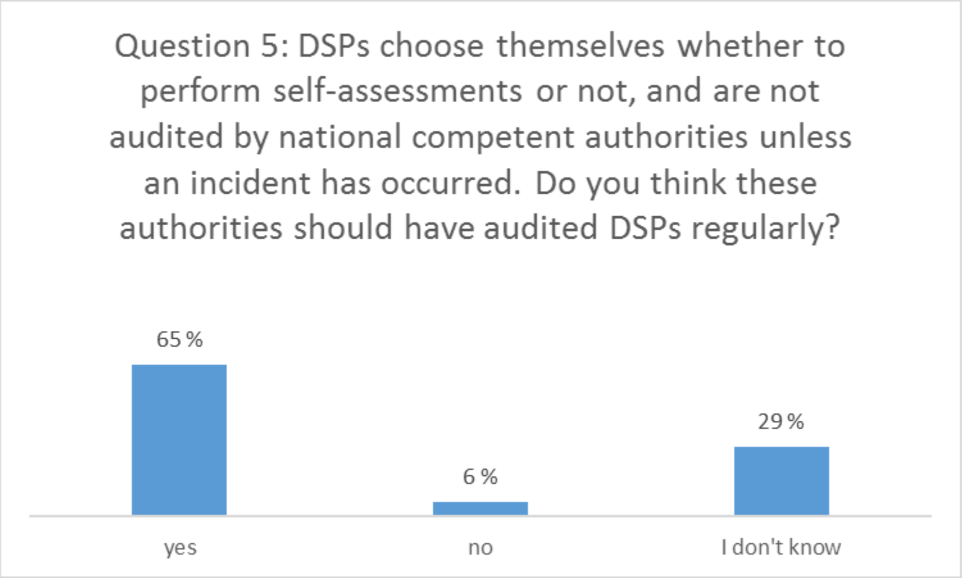
17 respondents working in the Governance, Risk and Compliance (GRC) and Technical Risk (TRS) departments.

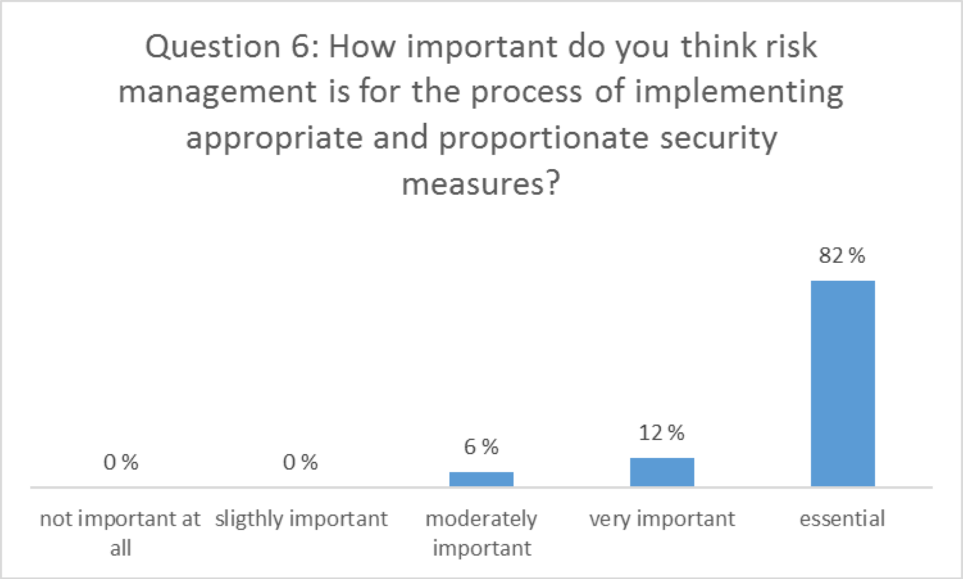


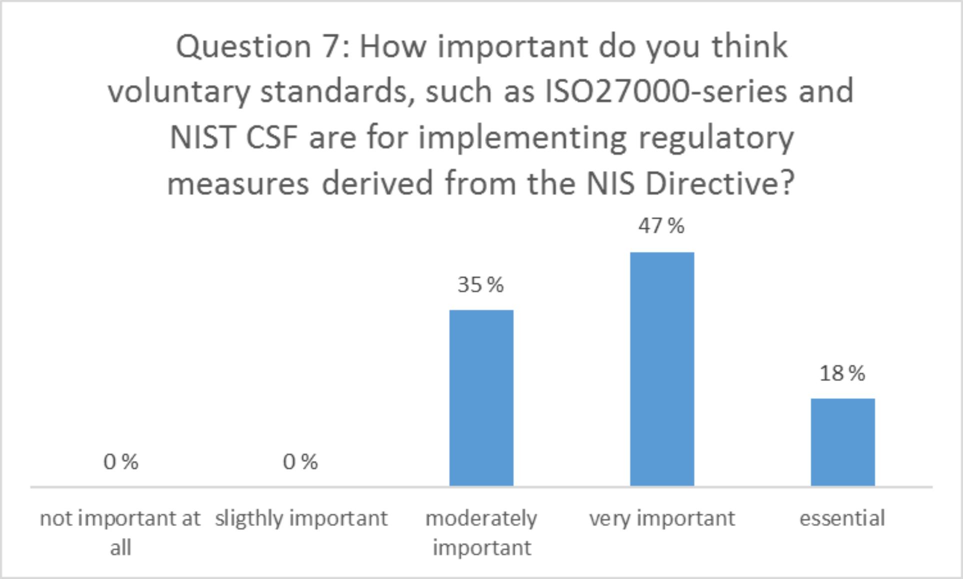


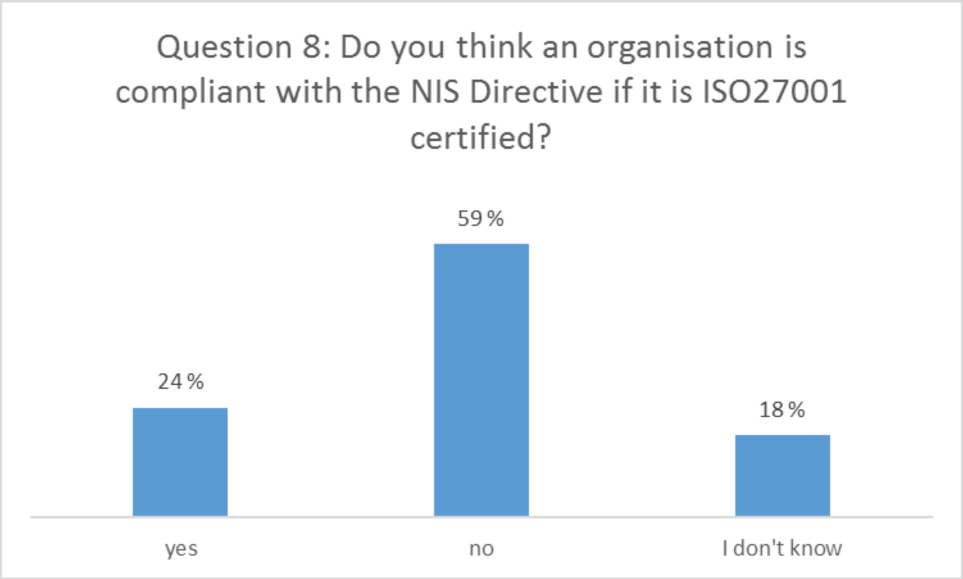

Question 3: How important do you think it is to impose strict security requirements on DSPs?

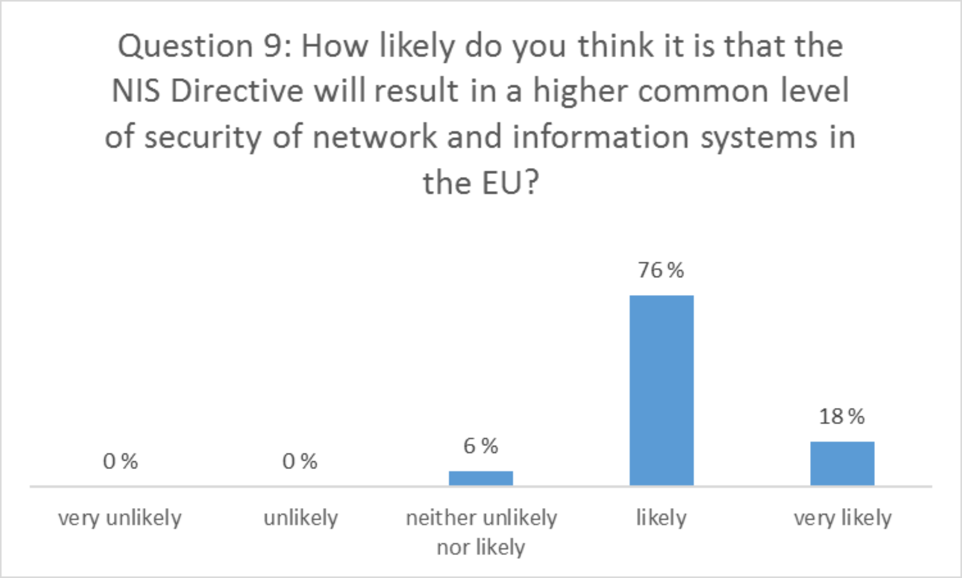

Question 4: How important do you think it is that OES are regularly audited by national competent authorities for its compliance with the NIS Directive?


Question 5: DSPs choose themselves whether to perform self-assessments or not, and are not audited by national competent authorities unless an incident has occurred. Do you think these authorities should have audited DSPs regularly?


Question 6: How important do you think risk management is for the process of implementing appropriate and proportionate security measures?


Question 7: How important do you think voluntary standards, such as ISO27000-series and NIST CSF are for implementing regulatory measures derived from the NIS Directive?


Question 8: Do you think an organisation is compliant with the NIS Directive if it is ISO27001 certified?



10 Annex III: phone interview with the Justice Department

Unofficial interview with the Senior Advisor in the Justice Department responsible for the implementation of the NIS Directive in Norway.

What is the progress of the implementation of the NIS Directive in Norway?
The implementation of the NIS Directive is a work in progress. The main focus now is to assess the scope of the Directive and to what extent Norway should harmonise the identification process with the Directive, or also include other sectors. There is an active discussion in this field at the moment.
What are the next steps?
The public review period is over, and the next step is to finalise the proposition before the lawmakers takes the proposition to debate. The Directive will possibly be adopted in 2020, no matter if it is a part of the EEA Agreement or not, which also Iceland is intending to do.
How does the Department work with the methodological approach in identification of OES?
National Security Agency (NSM) is mandated to establish a methodological approach in the identification of OES, like they have been doing with the Norwegian Security Act (Sikkerhetsloven). The methodological approach will also comprise of the application of thresholds in each sector, in which sectoral authorities and others shall be included in this capacity. The result of establishing a methodological approach will lead to a list which the organisation can apply

themselves in the assessment of whether they are covered by the legislation or not. The relationship between NSM and the Department is vital, although the specific departments responsible for critical sectors would have to take responsibility for identification when the Directive is implemented. Norway is also participating in the NIS Cooperation Group to exchange information and guidance on the subject of identification of OES.

What will be important to consider in the implementation of the Directive?

The Department consider it relevant to ensure a harmonisation to the greatest extent possible with the EU. There will be a national evaluation reflecting this topic after the evaluation from the EU is released. The Senior Adviser mentions that Norway is in a good position, as it can learn from the experiences on methodology across the Union, and try to avoid inconsistencies from the beginning.

How do you think the wording of security requirements should be adopted into Norwegian legislation?

The Department has not officially expressed an opinion on this matter, but the ambition is to create security requirements as similar to the Directive as possible.

11 Annex IV: Key findings from the NIS Directive Impact Assessment

In general, the respondents to the public consultation:

– Expressed the view that governments in the EU should do more to ensure a high level of NIS (82.8% of respondents)

– Expressed the view that users of information and systems are unaware of the existing NIS threats and incidents (82.8% of respondents) and that businesses, governments and consumers in the EU are not sufficiently aware of the behavior to be adopted to minimize the impact of the NIS risks they face (84%).

– Would in principle be favourable to the introduction of a regulatory requirement to manage NIS risks (66.3% of respondents) at EU level (84.8% of those respondents).

– Expressed the view that it would be important to adopt NIS requirements in particular in the following sectors: banking and finance (91.1% of respondents), energy (89.4%), transport (81.7%), health (89.4%), Internet services (89.1%), public administrations (87.5%).

– Expressed the view that requirement to adopt NIS risk management according to the state of the art would entail for them no additional significant costs (43.6%) or no additional costs at all (19.8%).

– Expressed the view that if a requirement to report NIS security breaches to the national competent authority were introduced, it should be set at EU level (65.1%) and affirmed that also public administrations should be subject to it (93.5%).

– Affirmed that a requirement to report security breaches would not cause significant additional costs (52.5%) and 19.8% said that it would not cause additional costs at all.

4.1.1. Disruptions to the EU internal market

Given that networks and information systems are interconnected and given the global nature of the Internet, many NIS incidents transcend national borders and undermine the functioning of the internal market.

The effects of an incident originating in a particular country, if not appropriately contained, may spread quickly to other countries. Even, incidents that are local by nature may have unforeseen consequences across borders, e.g. the disruption to a major airport's IT systems may affect air traffic across Europe.

4.1.2. Rising number, frequency and complexity of NIS incidents, and incomplete view of their frequency and gravity

The availability, authenticity, integrity and confidentiality of information and networks can be compromised due to various causes, such as natural events, human errors or malicious attacks.

The outcome of the public consultation confirms the seriousness of the problem, in particular:

56.8% of the respondents reported having experienced over the last year NIS incidents (caused by human mistakes, natural events, technical failures or malicious attacks) which have had a serious impact on their activities.

27.8% of the respondents to the public consultation affirm that human/technical errors are very frequently the cause of NIS incidents, and 39.6% affirm that this is the case quite frequently.

40.8% of the respondents to the public consultation affirm that malicious attacks are quite frequently the cause of NIS incidents.

36.1% of the respondents to the public consultation affirm that software/hardware failure is quite frequently the cause of NIS incidents.

47.3% of the respondents to the public consultation affirm that third party/external failure is quite frequently the cause of NIS incidents.

4.1.4. Sectors where the well-functioning of network and information security is key to preserve the well-functioning of the internal market

The public consultation underlined the importance of ensuring the security of network and information systems, in particular for the following sectors:

· Energy – 89.4% of respondents

· Transport - 81.7% of respondents

· Banking and finance – 91.1% of respondents

· Health – 89.4% of respondents

· Internet services – 89.1% of respondents

· Public administrations –87.5% of respondents

At the same time, 31% of respondents (both business and consumers) to the public consultation affirmed to have no process in place to manage NIS risks. Also, 54.2% affirmed not to have any budget dedicated to NIS.

All the sectors, which provide services which are key for the functioning of our economies and well-being of our society, rely heavily on network and information systems.

4.1.5. What will happen if further measures are not adopted

4.1.5.1. Undermined consumer confidence in the internal market

The number of NIS incidents and their negative consequences will continue to increase and this will have a negative effect on the use of online public and private services, on consumers' trust in the on-line economy and in the integrity of the Internal Market.

The 2012 Eurobarometer on cyber-security found that 38% of users had concerns with the safety of on-line payments and have changed their behaviour because of concerns with security issues: 18% are less likely to buy goods on-line and 15% are less likely to use on-line banking[34]. The perceived lack of security on the Internet is thus having a negative effect on the functioning and development of the Internal Market. It is estimated that, by stimulating the development of the digital single market, Europe could gain 4% GDP by 2020[35]. This GDP increase corresponds to a gain of almost €500 billion (€494 billion) or more than €1.000 for every citizen. In a time of economic downturn, this is not negligible.