First supervisor: Dr. Zlatina Georgieva, Utrecht University

Second supervisor: Dr. Tobias Theiler, University College Dublin

The Dutch Critical Infrastructure under NIS2 Directive:

A Cybersecurity Risk-management Approach

By: Virginia González Pouso

MSc European Governance

v.gonzalezpouso@students.uu.nl

Universiteteit Utrecht (2534703)

University College Dublin (21207764)

Abstract

Digitalisation is currently a hot topic in the EU and the Netherlands specifically, as EU-level NIS and NIS2 Directives have arisen to achieve a high level of cybersecurity. However, these directives and the speed at which they must be met are a double-edged sword. Though it allows for better connections and eases in monitoring the daily online activity of Member States that share a common interest in cybersecurity, the regulations are rather slow to adapt to the quickly changing nature of ICT systems. Further, every Member State has different levels of digitalisation and different resources at its disposal to reach and maintain a high common level of digitalisation.

To ensure the uninterrupted provision of vital services such as transportation and digital infrastructure, it is imperative that the critical infrastructure of EU Member States is prepared to confront cyber-attacks, system vulnerabilities, and risks in the digital domain. The implementation of a robust and actively enforced risk-management framework plays a crucial role in this regard. When essential processes like electricity or water supply, management of shipping traffic, or payment transactions become targets, society can be brought to a standstill for an unknown period of time.

In light of this, the EU legislative framework tries to be updated to present times after different digital proposals such as NIS (1&2), CER, CRA, or DORA, but there is often a misunderstanding of what these laws mean in practice and what extent national entities are responsible for implementing them.

This research work explores the extent to which cybersecurity risk-management measures in light of the NIS2 Directive are effectively monitored, developed, and practiced by Dutch governmental entities, as well as private organisations' effect on the public enforcement of the measures, and the extent to which these measures are complied with in practice. Lastly, this research work comes up with policy recommendations to address the challenges encountered in practice.

Key words: cybersecurity risk-managament, implementation, NIS2 Directive, critical infrastructure, transportation, digital infrastructure.

Acknowledgments

I am grateful to all of those with whom I have had the pleasure to work with during this research work. First, I am profoundly grateful to my supervisor Pei-Hui Lin in the Risk Management and Cybersecurity research group at the Centre of Expertise Cyber Security at the Hague University of Applied Sciences. Secondly, I am grateful for my supervisor's feedback and support in shaping this thesis.

I extend my appreciation to my parents and friends, whose unwavering support has been instrumental in bringing this research work to fruition.

TABLE OF CONTENTS

Abbreviations

Bbni: Network and Information Systems Security Decree *(Besluit beveiliging network- en informatiesystemen)*

CER: Directive on the resilience of critical entities

CISOs: Chief Information Security Officer

CRA: Cyber Resilience Act

CSAN: Cyber Security Assessment Netherlands 2022

CSIRTs: Computer Security Incident Response Team

CVD: Coordinated Vulnerability Disclosure

DORA: The Digital Operational Resilience Act

DTC: Digital Trust Centre

ENISA: European Union Agency for Cybersecurity

IBRA: the Inspection-wide Risk Analysis (*ILT-brede risicoanalyse*)

ICT: Information and Communications Technology

IJeV: Justice and Security Inspectorate *(Inspectie Justitie en Veiligheid)*

ILT: Human Environment and Transport Inspectorate

ISACs: Information Sharing and Analysis Centres

ISMS: Information Security Management System

ISO: International Organisation for Standardisation

NCSC: National Cyber Security Centre

NCTV: National Coordinator for Security and Counterterrorism

NIS Directive: Directive concerning measures for a high common level of security of network and information systems across the Union.

NIS2 Directive: Directive on measures for a high common level of cybersecurity across the Union.

NIST: National Institute of Standards and Technology

RDI: Dutch Authority for Critical Infrastructure

Wbni: Network and Information Systems Security Decree *(Wet Beveiliging network- en informatiesystemen)*

Chapter 1. Introduction

Our society is highly digitised, and business and private users utilise various IT applications daily. Consequently, our daily life activities are monitored in cyberspace and cyber-risks occur among other things because of the vulnerable computer equipment of private and public organisations, governmental institutions, and the general public as well. As a result, these vulnerabilities are especially important when it comes to critical infrastructure because that infrastructure is becoming the main target of cyber-attacks and the sectors at stake are still in need of more cybersecurity risk-management measures, increase the number of resources to tackle cyber-risks, and collaborative information sharing procedures. In this regard, the critical infrastructure of EU Member States should be ready to tackle cyber-attacks, systems' vulnerabilities, and risks in cyberspace, because a well-designed and actively applied risk-management framework contributes to guaranteeing the continuity of essential services such as transportation or digital infrastructure, among others (IJenV, 2022, p. 10). Therefore, information sharing both nationally and internationally is essential to mitigate risks among other measures that can be taken into consideration by the governmental institutions of Member States. Digital security forms an integral part of national security. For instance, when vital processes such as the electricity or drinking-water supply, the handling of shipping traffic, or payment transactions are being targeted, society can be brought to a standstill for a non-specific period (CSAN, 2022, p.15).

It is fundamentally important to implement from within governmental institutions, organisations, and stakeholders a model that helps to provide society with the necessary information to overcome future threats because a system that does not have security measures up-to-date can compromise the cybersecurity of an entire organisation while being online. Consequently, among others, the organisation establishes codes of conduct, builds employees' resilience, and raises awareness about caution in online interactions (Strupczewski, 2021, p.2). Thus, while organisations are trying to improve their cybersecurity, more should be done to make information and communication technology (ICT) systems resilient and ready before perceiving an attack, meaning that the risk-management procedure needs to be covered beforehand by identifying the threats, analysing how these threats could potentially penetrate in IT systems and consequently, stimulate cyber-performance of the entities by continuous detection and improvement

activities with the main goal of protecting IT assets and services for future risks (Lee, 2021, pp. 663, 668-670).

The application of Directive 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) and Directive 2016/1148 (NIS Directive) before that, comes as a response to building cybersecurity capabilities across the Union. Moreover, it tries to mitigate threats to network and information systems used to provide essential services in key sectors heavily dependent on ICT services. The periodic review process developed by the original NIS Directive has revealed inherent shortcomings that prevent it from effectively addressing current and emerging cybersecurity challenges. The proposed expansion of the scope covered by NIS2 Directive includes effective obligations for more organisations to take cybersecurity risk-management measures to reduce threats, incidents, and risks and ultimately, to increase the level of cybersecurity in the EU in the long run (Directive 2016/1148, Directive 2022/2555). The Directive urges Member States to speed up the setting-up of already existing computer emergency response teams (CERTs) as computer security incident response teams (CSIRTs), to which businesses and consumers can report malicious emails and websites. For instance, the National Cyber Security Centre (NCSC) has non-stop assistance for reporting cyber-incidents in the Netherlands. Moreover, throughout Europe, there are Information Sharing and Analysis Centers (ISACs). These non-profit organisations are not named in the Directives per se, but depending on the Member State they can receive different denominations. They provide a central resource for gathering information on cyber-threats (in many cases to critical infrastructure) while allowing for sharing of information between the private and the public sector about incidents and threats, sharing knowledge and analysis.

This research focuses on the case study of the Netherlands and the implementation of the NIS2 Directive in the context of the Dutch critical infrastructure, more specifically, analysing the procedural and enforcement effectiveness of cybersecurity risk-management measures. The study specifically zooms in on the Directive's provisions on *cybersecurity risk-management* (Article 21(2)(f)) because the Directive does not provide a concrete definition of the term in its Article 6, although it is of critical importance. Therefore, Member States need to specify what they understand under 'cybersecurity risk-management measures' and how *they* are going to be implemented in their national legislation. Subsequently, the sectors of high criticality as stipulated in Annex 1 of the

NIS2 Directive need to comply with those measures. Thus, the practical consequences that the implementation of these measures have in Dutch critical infrastructure are still to be analysed, which allows for this research to take place.

This reseach aims to assess the implementation of the NIS2 Directive in the Netherlands. According to the Head of Digital Resilience of the Dutch Authority for Digital Infrastructure, Jasper Nagtegaal, the Dutch approach to the NIS and NIS2 Directives is adequate, since all means are in place and there is enforcement by different supervisory authorities, implying that other Member States are not in that same position just yet (Secura, 2022). For this reason, the Netherlands is considered a leader in cybersecurity within the European Union and it is interesting and important to see whether the Dutch approach to the implementation of the NIS2 Directive is indeed 'adequate'.

1.1. Justification

This research topic has been chosen for various reasons. Firstly, the procedural and enforcement effectiveness of cybersecurity risk-management measures has not been studied before and also these measures are stipulated for the first time in the NIS2 Directive. Secondly, the Netherlands is a highly digitised country, being a world-class hub in Europe and one of the most digitised countries in the world, which offers many opportunities, but also brings risks that need to be assessed and monitored (CSR, 2022, p.25; NCTV, 2022, p. 7). Thirdly, in the Netherlands, there are a lot of cybercrime activities due to playing an important role in the Internet infrastructure (Leukfeldt, 2017, p. 46).

Consequently, this topic is up-to-date with the current EU legislation and cybersecurity approach that the Netherlands has taken while exposing that cybersecurity is continuously evolving and therefore the process of cybersecurity risk-management measures needs to be dynamic and react in time to potential threats that may arise (Refsdal *et al.,* 2015, p. 46). Lastly, it has been seeing a high proliferation of Anglo-Saxon countries on the topic of cybersecurity risk-management, such as the US, UK, Canada Australia, New Zealand, and France. However, the Dutch case has been understudied, which allows for this research to take place.

It has been argued that securing cyberspace challenges has an influence on the organisation of political authority by sovereign nation-states. Whereas threats to national

security call for collectively binding decisions controlled by legitimate force, the state itself is regarded as largely incapable of providing cybersecurity (Weiss & Jankauskas, 2018, p. 260). This is the case because cybersecurity knows no borders, in cyberspace a multitude of actors are involved in the process which makes it more difficult for the government to keep control of the measures. For instance, multinationals might have their headquarters located in different countries and this has an impact on the rules and policies they need to obey as well as the extent to which systems are secure. Moreover, the resources that countries use for the protection of their systems might be scarce.

The 2017 WannaCry and NotPetya attacks caused a great deal of damage for numerous actors notably through the disruption of international logistics. Beyond direct disruption, there is also a concern that cyber-incidents erode trust in the single market which could hamper trade and would also have negative consequences in the long run for the growth and competitiveness of the European cybersecurity industry (Timmers, 2018, p. 364).
Other attacks such as the malware attack on Maastricht University in 2019 and the attack on the shipping and transport giant Maersk in 2017, showed that cyber incidents can be impactful on business operations and, consequently have an even higher impact on uncertainty. For instance, after the Maersk cyber-incident, the APM Terminals in Rotterdam were out of service, for which ships needed to divert and trucks to cause a traffic jam at the port and on the highway (Groenendaal, 2020). Cybersecurity knows no borders, cybersecurity issues have impacts online but also in the physical domain, e.g., communication processes, transportation, critical infrastructure, or supply chain. For this, the governance of cybersecurity risk-management in a country is key.

Consequently, analysing the future implementation of the NIS2 Directive in the Netherlands is relevant, because the Netherlands still needs to pursue concrete action plans: i) to be secure; ii) stipulate what the cybersecurity risk-management measures it will take; iii) avoid future risks in the online systems of stakeholders. Furthermore, in the Netherlands the estimated increase in the number of organisations due to the NIS2 Directive transposition into national law is from 300 to almost 5000 entities (CSR, 2022; NCTV, 2022, p.29). Consequently, this case study could allow for a more in-depth analysis of the cybersecurity risk-management measures and their implementation in the long run. Moreover, this study is focusing on the sectors of high criticality as stipulated in the NIS2 Directive (Annex 1): digital, transportation, and public administration, given

that these sectors still need more resources to implement cybersecurity risk-management measures to tackle cybersecurity risks (NCTV, 2022, p.26) (see Appendix A and B for further information on the Dutch critical infrastructure, and sectors of high criticality).

Overall, the high connectedness of critical infrastructure increases the possibility of damages or perturbations in the long run and this can have consequences in the Netherlands and abroad (Weiss & Jankauskas, 2018, p.262). Furthermore, the results achieved with this research can be generalised to other contexts of alike EU Member States, e.g., the founding states of the European Union, because among other reasons these Member States have similar legislative landscapes, which allows for replication of the results obtained with this research.

Given the above delimitations, this research aims to assess the implementation of the NIS2 Directive in the Netherlands and its performance regarding enhancing the procedural and enforcement effectiveness of the cybersecurity risk-management measures among governmental institutions in sectors of high criticality (the concept of effectiveness is explained in section *'Theoretical Framework'* below). Moreover, the public-private sector partnerships are going to be considered as well, because of the impact that the private sector has on the governmental enforcement of measures.

Lastly, concepts such as risks, incidents, cybersecurity risk-management framework, and cybersecurity risk-management measures are relevant since all are the cornerstone of this research. These terms will be defined in Chapter 3.

1.2. Research questions

The research question proposed hereafter seeks to analyse the procedural and enforcement effectiveness of cybersecurity risk-management measures as stipulated in the NIS2 Directive in EU Member States' governmental institutions, more specifically, using the case study of the Netherlands. Accordingly, the two central research questions are as follows:

- What is the approach followed by the Dutch governmental institutions to ensure compliance with the NIS2 Directive and how does this contribute to the effectiveness of cybersecurity risk-management measures in the Netherlands?

- To what extent is there room for improvement, in light of the principles of procedural and enforcement effectiveness?

Consequently, the following sub-questions to the research question arise:

- What is, (also according to the competent authorities), the definition of cybersecurity risk-management as interpreted in light of the NIS2 Directive?
- What are, (also according to the competent authorities), the risk-management measures as interpreted in light of the NIS2 Directive?
- What risks concerning effective enforcement do the competent authorities envision and how do they plan to effectively supervise (or monitor) the cybersecurity risk-management measures of the NIS2 Directive?
- What differences and similarities have been identified in the approach of the Dutch governmental institutions towards the implementation of cybersecurity risk-management measures of the NIS2 Directive?
- To what extent do the Dutch governmental institutions uniformly implement the Directive's cybersecurity risk-management measures?

Chapter 2. Theoretical framework

2.1.Introduction

This research seeks to analyse the procedural and enforcement effectiveness of the cybersecurity risk-management measures as stipulated in the NIS2 Directive. Therefore, this section outlines the effectiveness framework that provides the theoretical underpinning of this research. This research considers the effectiveness framework as follows: Member States should be the guarantors of their competent authorities' effective supervision and compliance with the NIS2 Directive (Directive 2022/2555, article 31(1)). Before delving into the broad concept of effectiveness, it is important to note that compliance or enforcement effectiveness differs regarding the implementation process depending on the view of lawyers and policymakers, since both groups of people speak different languages and have different views on the transposition processes in general (Mantenbroek, 2009, p. 28), and regarding the NIS and NIS2 Directives in particular. Therefore, problems with compliance or enforcement effectiveness might be the result of misunderstandings among different shareholders involved in the process of the

transposition into national law (Mantenbroek, 2009, p. 30). This research will pin point in the term '*enforcement effectiveness'*, since the term compliance broadens up the scope of the research. However, the term compliance is widely used in practice for different issues and problems encountered. Compliance is about following all types of rules (moral norms, soft laws), while enforcement is about hard law only (the NIS2 Directive). Consequently, the term compliance is considered as a precodintion or general principle for the theoretical framework of this research work that will be further explained below.

2.2. Effectiveness in EU cybersecurity legal framework

The concept of effectiveness is broad. Consequently, this research will focus on procedural and enforcement effectiveness. However, it is relevant to stipulate beforehand that in this research both concepts of effectiveness measure the process of implementation of the NIS2 Directive in the Dutch critical infrastructure, rather than just measuring a specific outcome. This is the case, because the NIS2 Directive is still in the process of being transposed into national law, thus when data about the NIS2 Directive is not available, the basis of the NIS Directive will be considered. Therefore, different measures are being taken into account when assessing these types of effectiveness. These measures do not encapsulate all the possible measures, but the ones considered to be relevant based on the empirical research as well as the ones that come across in the legal documents. Lavenex and Krizic (2022, pp. 42-43) explain the term effectiveness as a 'goal attainment approach' that has two different dimensions: policy output or *procedural effectiveness* and policy outcome or *enforcement effectiveness*. By focusing on these two types of effectiveness I can study and/or measure the implementation of the Directive concerning cybersecurity risk-management and come up with policy recommendations afterward.

Cybersecurity risk-management needs to address both technical and human aspects holistically, because cyber-threats and incidents do not only cause harm online, but can also cause physical harm, including harm to life, health, and the environment (Lee, 2021, p.661; Refsdal *et al.*, 2015, p. 37). The cybersecurity risk-management framework has different steps of which cybersecurity risk-assessment plays a central role in risk-management framework, meaning that the prior knowledge that the organisation has regarding the types of assets to be protected as well as the type of vulnerabilities and threats of the systems is relevant (Lee, 2021, p. 664). Thus, the cybersecurity risk-management framework must comply with basic principles such as creating and

protecting value, being an integral part of all organisational processes, being part of decision-making, or being based on the best-updated information on the topic. Secondly, organisations should establish procedures for how to support any of the processes of the overall risk-management, e.g., ensuring that different areas of expertise are brought together during risk assessments, that the interests of all relevant stakeholders are considered, that the risk evaluation criteria are appropriate and that the decision-making is informed (Refsdal *et al.,* 2015, pp. 12, 14). Consequently, information sharing both nationally and at the EU level is crucial when assessing cybersecurity risk-management framework across high-criticality sectors. Certain factors have been considered relevant for both procedural and enforcement effectiveness in this research work (see Table 1 below). These factors need general principles or preconditions to be fulfilled for both procedural and enforcement effectiveness to happen in practice in the Netherlands (see Table 2 below).

Table 1. Factors of procedural and enforcement effectiveness

Procedural effectiveness	Enforcement effectiveness
Information sharing nationally	Personal and institutional liability
Information sharing at EU level	Repellent enough to cyber-risks
Coordination/cooperation nationally	Resources to fulfil the objectives
Cross-border cooperation	Lessons learned from the predecessor – the NIS Directive
Public-private sector cooperation	Uniformity

Table 2. General principles or preconditions for procedural and enforcement effectiveness

Compliance
Risk-based approach
Trust
Harmonisation

Before delving into the factors for both procedural and enforcement effectiveness, this study will zoom in on the preconditions for the effectiveness framework to happen in the Netherlands regarding the implementation of the cybersecurity risk-management measures in light of the NIS2 Directive. This study understands these preconditions as the ones that need to be achieved before achieving the factors that will be explained after.

a) Compliance

Firstly, compliance is a precondition for both procedural and enforcement effectiveness to happen in practice. This is the case because the term compliance is widely used in the literature and practice. According to Chiti (2018, p. 60), enforcement should be considered as a complex process encapsulating specific strategies, based on normative preferences. Moreover, the process of enforcement is seen as the one that helps in implementing procedures oriented to achieve compliance through negotiation and problem-solving and these procedures vary on a case-by-case basis. The author sustains that the enforcement process relies on i) collaboration between the entities involved, thus implementing procedures may be seen as proactive instruments to ensure that the objectives sought are oriented to sustain ongoing dialogue between the actors, prevent problems from arising, and ultimately promote compliance; ii) the traditional tools of administrative and judicial control and sanction, which operate as instruments to enforce the implementing procedures/arrangements as stipulated in accordance to EU law. The result is a double-edged enforcement strategy, oriented to both face infringements and to solve compliance problems, but also to prevent such problems and to promote appropriate compliance procedures (Chiti, 2018, p. 61). When it comes to compliance, in both interviews and conferences attended, being compliant with standards was under debate. The debate was twofold. Firstly, whether complying with standards such as ISO or NIST was enough to be cyber-secure. Second, whether compliance was about checking boxes.

In practice, standards such as ISO and NIST are taken into consideration, and even it has been argued that ISO standards allow for a least burdensome approach in auditing when dealing with less mature organisations, meaning those organisations that do not have the resources, the capacity or the knowledge on cybersecurity risk-management, but that are under the scope of the NIS2 Directive, can take into account the aforementioned

standards.[1] The main point taken is that being driven by these standards is easier for medium-sized organisations and larger organisations, because those standards are rather easily understandable and allow to follow best practices in the industry; while at the same time are understood internationally for which cases of industries that operate in different countries might make their security easier.[2]

b) Risk-based approach

Secondly, the state-of-the-art as stipulated in the NIS2 Directive is a risk-based approach, which means that it should be ensured a level of security network and information systems appropriate to the risks encountered (Directive 2022/2555, article 21(1)). Also, 'the provider should prepare a risk analysis in which it describes the risks related to security and addresses how it reduces the risks by justifying what levels are considered appropriate. This just needs to address organisation-specific and sector-specific risks, the public interest of its essential service, and the state-of-the-art, thus the results of this document should be in security and control measures (Bbni, 2023, article 9.1).[3] Consequently, the term risk-based approach or proactive approach means that the risks that a specific organisation faces are a priorioty, for which that organisation will develop processes, procedures and policies to tackle/reduce that specific risk and lower its impact.

Some scholars have discussed the risk-based approach of cybersecurity thoroughly, not only in the public sector but also in the private sector. Bromiley *et al* (2014) discuss in their paper that prescriptions on risk-management often talk about firms adopting 'appropriate risk cultures' and that the idea of implementing risk-management comes from external actors in the first place (Bromiley *et al.*, 2014, pp. 268-269, 272). In the EU, the shift towards a more risk-based cybersecurity approach has been accompanied by several areas of Member State contestation, including the extent of EU involvement in operational cybersecurity activities and cyber crisis management efforts, as well as the issues of cybersecurity information sharing and incident reporting duties.

[1] Further information regarding the standards will be provided in Chapters 4 and 5.
[2] Therefore a centralisation of policies and procedures facilitates the work of multinationals, telecoms and other organisations with a rather internationalised scope, even though the headquarters are in the Netherlands (Second NISDUC Conference, 2023).
[3] *Besluit beveiliging network- en informatiesystemen* in Dutch.

This debate shows that the EU still faces certain challenges regarding cybersecurity risk-management approaches. Firstly, the disparity of Member State cybersecurity maturity levels when implementing or transposing the EU Directives into national law (Backman, 2022, p. 98). Secondly, the rapid change in technology development has consequences for the EU cybersecurity policy, since not all sectors are at the same level of maturity, e.g., sectors such as finance are mature in cybersecurity, while sectors such as energy and aviation are catching up, but other high critical sectors such as healthcare are lagging in cybersecurity measures (Timmers, 2018, p. 379; Backman, 2022, p.99). With the adoption of the Cyber Resilience Act (CRA) and the adoption of the NIS and NIS2 Directives, it can be said that the extent of the Member State's acceptance of a more risk-based cybersecurity approach is imminent due to the policies set out in the new EU cybersecurity strategy (Backman, 2022, p. 97). In this regard and for this study, it is interesting to analyse how the sectors that are catching up in cybersecurity are dealing with the national implementation process, not only from the supervision side but also from the private sector side. This will be further explained in the *'Procedural effectiveness'* section below.

The debate between compliance and risk-driven approach in cybersecurity risk-management has been further discussed in the Second NISDUC Conference,[4] because the maturity levels of different countries and organisations are different and compliance is not seen as the path to follow by many, since complying with standards does not mean being secure in cyberspace. There is a need for group effort as well as a proactive approach towards risk-management, an approach in which factors that will be further discussed in the *'Procedural effectiveness'* section such as cross-sector, public-private, and cross-border cooperation/collaboration are key; as well as, being repellent to cyber-risks or the resources at their disposal (discussed in *'Enforcement effectiveness'* section) In addition, the debate goes to platforms such as Linkedln. According to Weber (2023), without compliance, most companies would not even have the basics like incident and crisis management. Secondly, if compliance is just checking in boxes, it is implemented wrong. No tool can provide 100% of security. Finally, compliance is not the ultimate goal, the ultimate goal is security, therefore you use compliance to fill certain gaps and

[4] I attended the *Second NISDUC Conference: From NIS to NIS 2.0 a path to take* in Brussels on the 25th and 26th of April. Therefore, during those days I took notes of the insigths provided. See: https://www.nisduc.eu/second-conference

improve your approach. Overall, Weber (2023) emphasises the idea that compliance is the first step of many more, but complementary support, collaboration, sharing of knowledge, and stopping the narrow-minded view on topics such as compliance vs. cybersecurity is needed.

Overall, the debate risk-based vs. compliance is a debate still ongoing (see Appendix C for further information). In this regard, one main finding is that to a certain extent compliance and risk-based approach are seen as juxtaposed and other times are seen as the same thing. Therefore, it has been highly debated that being certified does not mean being secure and as an entity, you follow a risk-based approach and once you have come up with it, supervisory authorities check your compliance with the thresholds imposed by law. However, it seems that there is a misunderstanding of the concepts and that these two concepts have been used indistinctively. Therefore, understanding both seems key to be able to assess whether or not the procedures followed in the Netherlands are proactive or more about checking boxes. Either way, it seems this debate is not about a neither-or type of scenario, but that everything needs to be taken into account with the goal in mind of being resilient, aware, and secure.

c) Trust

Thirdly, trust is another precondition to the theoretical framework of effectiveness. This is a widely used term in politics and practice. With everything that happens in cyberspace, all types of trust are key for both regulators and regulatees. This study understands that trust is not just a matter of vertical relations between citizens and public authorities. Instead, attention should also be given to horizontal trust relationships between actors that are part of the rule-making process, such as public administration, the Dutch government, and so on (Tigre, 2021a, p.1). In the relationship between regulatory agencies and regulatees, trust in regulatory agencies is important to increase their effectiveness, because with low levels of trust in regulatory agencies are important to increase their effectiveness (Tigre, 2021b, p. 5). Moreover, a trustworthy relationship allows for information-sharing schemes among others, which will be further analysed in Chapter 5. Therefore, trust in the system is aimed for in practice.

d) Harmonisation

Lastly, this research understands harmonisation as a precondition when it comes to procedural and enforcement effectiveness. This is the case, because the Dutch governmental institutions, and the national actors involved in cybersecurity risk-management measures need to harmonise their approaches nationally. In this regard, according to Windholz (2012, p.326), there are four domains of harmonisation and the actors involved in the process of cybersecurity risk-management both in the Netherlands and at the EU level require to balance the interests, measures, and policies. Harmonisation is a complex term because of its interrelated policy issues, e.g., it is related to the process of the policies and also the uniformity of the policies in place (Windholz, 2012, p. 337). Therefore, this study understands harmonisation as the balancing measures that the Dutch governmental institutions, and more concretely, the sectoral ministries are taking regarding cybersecurity risk-management measures and to what extent they are being uniform in their approaches within the Dutch government.

Overall, these four preconditions are considered key for both procedural and enforcement effectiveness to be materialised in the Dutch implementation of the NIS2 Directive. Therefore, this study tries to depict whether the Netherlands has in place these preconditions within organisations' approaches taken for these procedural and enforcement factors to happen. This study analyses the factors that will be further seen in the sections below and analysed in Chapter 5 through the interviews conducted. Since these preconditions were also named through the interviews.

2.2.1. Procedural effectiveness

According to Lavenex and Krizic (2022, p. 42), *procedural effectiveness* can be quantified in terms of volume, depth, coverage, and reach. This means that effectiveness is measured by the level of autonomy, decision-making, and cooperation processes of the policy at stake and between the actors involved. This is further analysed in this research by measuring the factors of information sharing, cooperation, and collaboration as well as risk analysis, since all of those allow for the measurement of the procedural effectiveness framework.

When reading the NIS2 Directive different organisations, entities, and concepts pop up, which can be hard to understand at first. Consequently, this research zooms in on those

considered key for the attainment of the ultimate goal of the Directive: a high common level of cybersecurity. This research work considers among *procedural effectiveness* the following factors taken from both the literature and the Directive's mandates (see Table 1): information sharing both nationally and at the EU level; coordination and/or cooperation nationally, cross-border as well as public and private sector cooperation (Directive 2016/1148, article 16; Directive 2022/2555, paragraph 121, Lavenex and Krizic (2022).

Firstly, the concept of information sharing is considered fundamental. In this regard, the Directive stipulates that the Member States' competent authorities should cooperate when it comes to information sharing with undue delay for the identification of critical entities, risks, cyber-threats, and incidents affecting critical entities, including both cybersecurity and physical measures taken by critical entities, as well as the outcome of the supervisory activities (NIS2 Directive, paragraph 30). This study understands information sharing both nationally and at the EU level. Therefore, the information-sharing schemes happening among governmental institutions and the private sector and within governmental institutions and institutions alike. While the information-sharing schemes at the EU level, which happen through networks such as ISACs or CSIRTs, but not only. The fact that the research question is about the implementation of the Directive at the national level, does not mean that the information-sharing schemes at the EU level need to be dropped out of this study. This is the case because high criticality sectors are highly interconnected since cybersecurity knows no borders, therefore what happens in one country matters for the rest of the Member States. Moreover, it is important to already stipulate that trust is indeed a precondition, meaning that a trustworthy network is key when dealing with information-sharing schemes and for them to happen, this will be further analysed in Chapter 5.

Secondly, the concept of cooperation is also fundamental to this research. This research understands cooperation in three ways: i) coordination/cooperation nationally; ii) cross-border cooperation; and, public-private cooperation. Coordination and cooperation nationally do not appear per se in the NIS2 Directive, but it is aimed so CSIRTs or Cooperation Group networks can work as expected at the EU level. Therefore national coordination and cooperation are up to the national competent authorities, but this is key for this study to analyse the implementation of the NIS2 Directive in the Netherlands.

Therefore, the coordination of the Dutch government and its sectoral ministries on the implementation of the NIS2 Directive, as well as the coordination in their approaches is fundamental in this research. Consequently, harmonisation works as a precondition for this factor as well as the other preconditions stipulated in this Chapter above.

Then, cross-border cooperation is put into practice by the Cooperation Group, the CSIRTs network, and EU-CyCLONe, all of which ultimately help Member States to support and facilitate strategic cooperation and the exchange of information, while strengthening trust and confidence among the Member States' organisations involved (NIS2 Directive, paragraph 64). In principle, EU-CyCLONe and the CSIRTs network should cooperate based on procedural arrangements that specify the details of that cooperation and avoid any duplication of tasks by defining the network's roles, means of cooperation, interactions with other actors, templates of information sharing as well as means of communication to make cooperation effective (NIS2 Directive, paragraphs 5, 68). Moreover, this Directive considers key to ensuring cross-border cooperation of Member States' relevant authorities as well as cross-sectoral cooperation (Directive 2022/2555, article 8(4)). Therefore, both the national and EU level are quite interrelated when it comes to cooperation. This is the case because Dutch entities are part of these networks and knowing that cybersecurity knows no borders, the more cooperation cross-borderly, the more reduction of cybersecurity risks and, consequently the more effective implementation of the Directive in the Netherlands. Moreover, the EU level needs to be analysed, because the main goal of cross-border cooperation is to help Member States to implement the Directive at the national level.

In addition, the public-private cooperation is considered key in this study, because the private sector has the resources and standards in place that are considered the basis to take into consideration and then the public sector follows upon these approaches (Directive 2022/2555, paragraph 55). Therefore, this study aims to analyse whether the private sector influences the enforcement of procedures and/or measures by the public sector. This will be further analysed in both Chapters 4 (*'Risk-management in practice'* section) and 5. In our empirical findings, we will check to what extent this cooperation framework envisioned in the Directive is truly embedded within the national enforcer's agenda/thinking about the implementation of the NIS2 Directive.

2.2.2. Enforcement effectiveness

According to Lavenex and Krizic (2022, pp. 42-43), *enforcement effectiveness* assesses whether the institution, in this case, the Dutch supervisory authorities, but also the Dutch governmental institutions, through its policy output affect the behaviour of its target group which is the sectors of high criticality, meaning that these sectors change their measures over time due to the new Directive. Therefore, this framework could potentially help to assess whether the sectors of high criticality can comply, and ultimately solve the problems that the NIS and NIS2 Directives create in the first place (Lavenex & Krizic, 2022, p. 43).

This research considers among the *enforcement effectiveness* the following factors taken from both the literature and the Directive (see Table 1): both personal and institutional liability, assessing whether the NIS2 Directive is repellent enough towards cyber-risks and incidents of ICT systems, evaluating the lessons learned from the predecessor - NIS Directive; as well as ensuring that national competent authorities, CSIRTs, and organisations, in general, have adequate resources to carry out, effectively and efficiently, the tasks assigned to them and to fulfill the objectives of the NIS2 Directive (Directive 2022/2555, article 8); and, uniformity as in ensuring legal certainty regarding cybersecurity risk-management measures and guaranteeing a consistent criterion for entities under the scope of NIS2 Directive (paragraph 7) but also on the 'uniform' approach by the Dutch government.

Firstly, personal and institutional liability is considered under the enforcement effectiveness framework because it is understood as a last-resort mechanism used by governmental entities, thus other control measures are considered before the actual fines come into place. The variety of cybersecurity institutional agreements across the Union is vast, which complicates further the situation since some organisations do not know whether they are liable under the new legal framework or there might be certain overlaps between these different frameworks. Furthermore, there exist differences across the Union in terms of the desired extent of EU involvement in Member State cybersecurity activities (Backman, 2022, p. 99), meaning that maturity levels, available resources, and risk/compliance-driven approaches might differ between Member States. Therefore, the resources of organisations might be a deterrent on whether or not maturity levels are considered.

Secondly, by being repellent enough to cyber-risks this study tries to depict if the measures stipulated in the Directive can allow for this to happen and therefore analysing whether the precondition of both risk-based approach and compliance are in place and happen in practice (Directive 2022/2555, paragraphs 29, 80 and 124).

Thirdly, the resources to fulfill the objectives of the Directive is considered key as well, because the resources that entities at the national and EU level have, will determine the level of maturity that can be fulfilled and therefore whether or not the approach is burdensome for them (Directive 2022/2555, article 7 and paragraph 46).

In addition, regarding the lessons learned from the predecessor NIS Directive, this study tries to analyse the shortcomings that have been experienced due to the implementation of the NIS Directive to be able to analyse what to continue using with the new NIS2 and what not (Directive 2022/2555, paragraph 2).

Lastly, uniformity refers to consistent approaches among Member States to the same issue: cybersecurity. This research will check whether the Netherlands does take alignment measures within its governmental institutions and, to a lesser extent, other organisations. This term refers to the harmonisation of measures by the Dutch government regarding cybersecurity risk-management measures and it comes as a result of whether or not procedural effectiveness is happening in the Netherlands.

Further analysis of all the factors and preconditions considered in the Theoretical framework of this research work will be provided in Chapter 5 when analysing the data gathered from the interviews and literature review.

2.3.Effectiveness and cybersecurity risk-management

With the increase in cybersecurity risks posed by cybercriminals and adversaries, organisations ought to increase their awareness of the cybersecurity changes and be able to respond to them effectively (Lee, 2021, p. 669). In the meantime, cybersecurity risk-management measures need to address both technical and human aspects holistically (Lee, 2021, p. 661). Therefore, *procedural* and *enforcement effectiveness* need to both be fulfilled to address cybersecurity risk-management in the Dutch critical infrastructure and to be replicable in other Member States' critical infrastructure as well. Consequently, this

research work will analyse whether both types of effectiveness, with factors and preconditions, are in place in the Netherlands in Chapter 5.

Regarding the cybersecurity risk-management measures, a proactive approach to cyber-threats is a vital component of cybersecurity risk-management. This should enable the competent authorities to effectively prevent cyber-threats from materialising into incidents that may cause considerable material or non-material damage while ensuring uniformity by harmonising these measures to be equally developed across high criticality sectors such as digital, transportation, and public administration sectors taken into consideration in this research (Directive 2022/2555, Annex 1).

Overall, the approach taken into consideration in the Directive aims for procedurally and enforcement-wise effective cybersecurity risk-management measures. However, these measures are not defined by the Directive itself. Therefore, this research will use the text of the NIS2 Directive, existing literature findings as well as the insights provided by the respondents to comprehend and analyse the cybersecurity risk-management framework. The said assessment will take place in the following sections which are structured as follows: methodology and research strategy (chapter 3), literature review (chapter 4), main empirical findings (chapter 5), the outcome of the research, and policy recommendations (chapter 6) and, lastly, conclusions and limitations of the study (chapter 7).

Chapter 3. Methodology

In this section, the methodology of this research is further explained. The whole process before and after conducting the interviews is also shared since it is fundamental to understand both the purpose and the process of this research, which will allow us to contextualise and validate the results achieved later on in this study.

This research work aims to answer the main research question by looking at EU cyber risk-management measures related to cyber-risks, threats, and incidents that occur in cyberspace. It also depicts the impact that this Directive has on Member State's governmental institutions, more concretely, considering the case of the Netherlands. Moreover, this study zooms in on cooperation and collaboration at the national level

among entities of different natures. In this regard, public-private partnerships are considered key in puzzles such as cybersecurity since they have resources and knowledge to spill. Consequently, the complex system of collaboration schemes needs to be taken into account when analysing issues such as the implementation of cybersecurity risk-management measures in the Netherlands.

This research follows the case study as a research method and interdisciplinary approach to be able to depict the most important information of a complex issue such as the procedural and enforcement effectiveness of cybersecurity risk-management measures in light of the NIS2 Directive in the case study of the Netherlands. Firstly, according to Yin (2009, pp. 4, 18-20), the case study research allows the researcher to understand complex real-life situations regarding the practical implementation of the NIS2 Directive in the Netherlands, because the boundaries between context (the implementation) and phenomena (unforeseen political, economic or social circumstances) are not clearly defined and multiple variables are at stake such as different actors, legal frameworks, rules, political agendas and cybersecurity strategies,[5] (Weiss & Jankauskas, 2018, p. 262). Thus trying to depict a useful overview by combining different strategies is the action taken in this research: (i) case study notes from interviews, observations, document analysis (Yin, 2009, p. 120), and conferences attended such as the Second NISDUC Conference (2023); (ii) case study documents related to the topic and stored electronically throughout the process; and, (iii) case study narratives, which are produced by the researcher once the data collection through the information provided in the interviews is completed, thus in the form of transcripts [6] (Yin, 2009, p. 121). Secondly, this research will be interdisciplinary because cybersecurity is a complex issue and it can be analysed through the lenses of the legal and political science disciplines (Repko & Szostak, 2021, p.84). The value of an interdisciplinary approach is that it can address complex problems such as procedural and enforcement effectiveness of cybersecurity risk-management measures in the Dutch critical infrastructure in a more comprehensive way. This is the

[5]Actors from the local, regional, national, and international levels, not only countries but also multinationals with a lot of power in the digital domain in cross-border activities; public and private organizations; citizens; IT developers; hackers, and so on. Legal frameworks at the EU level also at the international level, overlap, and in the cases of multinationals based in different countries can have an ethical impact. Different values, rules, political agendas, governance models, and cybersecurity strategies develop the cyber domain. Cybersecurity awareness levels as well as practices. Therefore, a lot of factors are at stake when analysing this topic.

[6] Transcripts of the interviews are available upon request to the writer of the thesis. The contact details are in the front page of this research work.

case because neither the political science discipline nor the legal discipline can deal solely with this complex issue. Therefore, the interdisciplinary combination of the two is necessary to reach a more comprehensive perspective (Repko & Szostak, 2021, p. 95). In this research work, we are using legal analysis when selecting the provision of the NIS2 Directive that are relevant to the research, while we use political science analysis when interpreting the empirical findings. By combining both the Dutch legal framework and political agenda in cybersecurity risk-management issues, this research will add a new perspective to the literature not studied before.

This study aims to analyse the procedural and enforcement effectiveness of cybersecurity risk-management measures in the Dutch critical infrastructure. Cybersecurity risk-management has been studied by scholars in different sectors and countries. With the increased cybersecurity risks posed by cybercriminals and adversaries, it became imperative for organisations to increase their awareness of the change in the cybersecurity landscape and respond to those changes effectively (Lee, 2021, p. 669). Therefore, analysing the implementation of cybersecurity risk-management by the Dutch governmental institutions (supervisory authorities and CSIRTs) as well as the private sector's impact on public enforcement is crucial in this research.

All in all, plenty of actors participate in cyberspace since the daily actions are digitalised, therefore the analysis of this interaction between the public enforcement and the private sector can benefit the outcome of the research, while allowing to test the theoretical framework that has been discussed in the section above.

3.1.Terminology

Before exposing the debates regarding the issue of cybersecurity risk-management measures and the sources of information, it is essential to provide the study with the definition of these measures and cyber-risks according to the NIS2 Directive, but also according to the literature. Cyber-risks are not defined in the Directive, but terms such as risks and incidents are. According to the Directive, an incident is an event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data or of the services of network and information systems (Directive 2022/2555, article 6(6)); while the term 'risk' is defined as the potential for loss of disruption caused by an incident and is to be expressed as a combination of both

the magnitude of the disruption and the likelihood of the incident to occur (Directive 2022/2555, article 6(9)). According to Refsdal *et al* (2015, pp. 31, 34), cyber-risk is understood as the union of malicious and non-malicious cyber-risks, and the cybersecurity risk-management is concerned with risks caused by cyber-threats.

In this research, cyber-risk is understood as a risk resulting from the possible intentional and unintentional damage to an ICT system, which threatens confidentiality, availability or integrity of digital data, information flow, and services. The damage leads to business interruption, infrastructure failure or other material damage and non-material damage such as privacy (Strupczewski, 2021; Directive 2022/2555, article 6(6),(9)). There are other conceptualisations of the term cyber-risk by ENISA Glossary or ISO 31000 (2018). However, this research will take into consideration the aforementioned conceptualisation because it is the definition derived from the Directive itself, it is the most specific regarding all the spheres to be taken into consideration when analysing risks in a broader context; and, other conceptualisations are too schematic and do not add enough information to the matter of the study.

Cybersecurity risk-management measures are the ones that essential entities need to implement in their ICT systems to fulfill certain standards at the EU level but also with standards recognised internationally such as ISO 27000 series, and NIST, among others. According to the NIS2 Directive, the cybersecurity risk-management measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, including policies on risk analysis and information system security; incident handling; business continuity (such as backup management and disaster recovery, and crisis management); supply chain security-related aspects; security in network and information systems including vulnerability handling and disclosure; policies and procedures to assess the effectiveness of cybersecurity risk-management measures; basic cyber hygiene practices and cybersecurity training; the use of multi-factor authentication and secured emergency communication systems within the entity (Directive 2022/2555, article 21(2)).

3.2.Research strategy

To answer the research question and sub-questions, I will conduct research through a qualitative analysis plan, retrieving data from different qualitative sources, such as academic reviews, national cybersecurity strategies, policy reports, and semi-structured interviews. To be able to answer the main questions, the steps to take are as follows.

Firstly, a separate analysis of both the literature review and the interviews is necessary to be able to assess what are the gaps that the interviews are filling. By doing this, concepts that are not being defined in the Directive, such as cybersecurity risk-management and cybersecurity risk-management measures can be further explained.

Secondly, the elements of the research will be taken altogether, making an overall assessment of both procedural and enforcement effectiveness of the Dutch competent authorities, private and public entities as well as EU entities for the sectors of high criticality of interest in this research. By doing this, a bigger picture can be developed, which will allow us to first analyse the broader context, followed by the EU context, and lastly, the more concrete context of the Dutch case. Even though the research question that this study tries to answer is the effectiveness (both procedural and enforcement) of the national implementation of the NIS2 Directive in the Netherlands, what happens at the EU level shapes the reality, and helps this implementation to take place through the different networks mentioned in the sections above.

Thirdly, I overlay my theoretical framework on the effectiveness with my empirical findings among Dutch governmental institutions and organisations within the sectors of high criticality, e.g., digital, transport, and public administration. This is assessed and further explained when conducting the semi-structured interviews. Because once all the interviews are done, the coding process can allow for an analysis of the respondents' approach to the implementation of cybersecurity measures in the Netherlands and to make conclusions regarding the effectiveness framework.

Lastly, based on effectiveness and as a matter of future assessment, all the information previously analysed, provides food for thought. Therefore, this study will aim for policy recommendations addressed to organisations in the Netherlands and the EU.

These methods have been chosen for various reasons. Firstly, the literature review allows for collecting data on cybersecurity risk-management previously analysed by experts. This enables contextualisation of the topic of cybersecurity. Moreover, the literature review can be beneficial when aiming to map the development of a particular research field over time, which adds value to this research in particular, because it provides the basis for identifying gaps and/or building a new conceptual model (Snyder, 2019, p. 334). In our research, we do the former. The literature review also enables to identify and, ultimately avoids bias that might be encountered when analysing political reports or governmental strategies, e.g., confirmation bias. The technique used in the literature review is the snowball effect, which implies using the reference list of a paper to collect other papers that might be of interest to this research (Wohlin, 2014, p.1).

Secondly, the usage of official publications of both Dutch cybersecurity strategies and policy reports enables the assessment of the particular action taken by the Netherlands to comply with cybersecurity risk-management measures as stipulated in the EU Directives. Thirdly, the interviews would follow a semi-structured format to provide a certain fixed outline to the interview while allowing for the flow of the conversation by asking follow-up questions (Aberbach & Rockman, 2002, p.675). Conducting interviews with officials from the competent national authorities allows us to measure unobservable data that will not be accessed otherwise while taking relevant insights for the research. The questions to ask will be grand tour questions, example questions, and prompt questions to allow for the flow of the conversation for the reasons aforementioned (Leech, 2002, p.667-668).

3.3.Sampling and data collection

This section will discuss the process of the data collection and the steps followed: selection of the sample for this research, contacting process, scheduling interviews, and sampling after the interviews were conducted.

Firstly, the selection of the sample for this research took me around three weeks from January until February. Since the beginning, the institutions of interest were governmental institutions. After further discussion with my supervisors, we also decided to consider respondents from the private sector, to establish contact with both ‘producers’

and ‘consumers’ of the law relevant in the Netherlands and thus to give different insights to the research. I have chosen a non-random sampling strategy.

The purpose of the semi-structured interviews was to develop causal explanations which generate particular outcomes. In this case, the analysis of both procedural and enforcement effectiveness of cybersecurity risk-management measures in the Dutch critical infrastructure is aided by this strategy. For this reason, the data gathered takes the form of ‘causal process observations’ defined as an ‘insight or piece of data that provides information about context, process or mechanism’ (Mosley, 2013, p. 19).

The time constraints and the answers received by respondents contacted to participate in the study had an impact on the strategy followed in this research. Consequently, the contacting process was made by both the institutional email (from the Centre of Expertise Cyber Security in the Hague University of Applied Sciences) and Linkedln (professional account). The main institutions that were contacted were national competent authorities under the scope of the NIS2 Directive in the Netherlands e.g., the regulatory bodies for the sectors of transport and digital. Firstly, the Human Environment and Transport Inspectorate (Patrick van de Heisteeg who is the coordinator advisor of cyber supervision in the Human Environment and Transport Inspectorate for the Netherlands). Secondly, the Dutch Authority for Digital Infrastructure. Thirdly, a cybersecurity-specialised organisation doing all sorts of cybersecurity consultancy and auditing. Moreover, the National Cyber Security Centre (NCSC). Furthermore, a private company from the aviation sector. In addition, the Permanent Representation of the Netherlands in the EU (Gijs Peeters). Also, the European Parliament; and, lastly, ENISA.

Secondly, both the contacting process and the scheduling of interviews took a total of three months (from February up until May). Because of the need to create a trust process, several getting-to-know meetings with certain institutions were needed, and there was one follow-up interview. From the emails sent, some institutions were not interested in participating in the research. In total, around thirty emails were sent and fifteen respondents were contacted separately through Linkedln. Overall, I have conducted eight interviews (see Appendix D).

Thirdly, greater transparency in the interview process will increase confidence in our findings and conclusions sections (Mosley, 2013, p. 20). The interviews lasted between 45 and one hour and a half in total. There has been one case, in which I conducted a

follow-up interview, thus for that interview, the time was almost two hours. This allowed me to be able to ask the core questions of the research as well as keep the flow of the conversation and become aware of the key components of how the transposition of the NIS2 Directive into national law works. Moreover, these interviews are anonymised for security purposes after signing a confidentiality agreement by the respondents (see Appendix E).

As it was aforementioned, when conducting the interviews a certain structure was followed but the flow of the conversation plus the specific sector or knowledge of the interviewee was considered (see Appendix F). For two of the interviews, there were several getting-to-know meetings beforehand which allow to establish a good groundwork to be able to have a more fruitful conversation.

Finally, once the interviews were conducted, the discourse analysis method is taken into consideration to look at what has been said in the interviews as well as what is implied by the answers given by the respondents (Manheim *et al*., 2012, p. 351, 360). Then, I created a coding tree with the concepts that were key to our interviews and that they emphasised and report the most (see Appendix G). This allows me to glimpse the concepts that were used more than once by the respondents. Thanks to the coding tree, I can determine which elements in the research were the dominant or relevant ones and which ones are not (Boeije, 2010, pp. 108-109). Coding is a method that enables one to organise and group similarly coded data into categories because they share some characteristics and after several rounds of coding, there might be some rearrangement and reclassification of coded data into different and even new categories (Saldaña, 2013, pp. 9, 11).

Before creating the coding tree, I put back together data with open coding after the interviews. I followed open-source coding, initial coding, and axial coding. This is the case because a first and second cycle of coding allows me to code processes from the beginning stages of data analysis and later on split the data into smaller coded segments (Saldaña, 2013 p. 52). While through the second cycle of coding, I can reorganise and reanalyse data coded at first which can be considered redundant or marginal during the second round (Saldaña, 2013, p. 207). As a result, the coding tree displays in a simple way the process of codes and subcodes that summarise the main clusters of ideas gathered in the interviews and after the three phases of coding. During the axial coding phase as

well as the transcription of the interviews, I made use of the discourse analysis method that not only looks at what has been said in the interviews but also what is implied by what has been said by the respondents which is also known as subtext analysis. Consequently, this allows me to associate words and concepts used by the respondents with their views and perception on the usage of words, and ultimately this led me to explore potential assumptions about the nature of political relationships of the respondents with EU Directives, more specifically, the NIS2 Directive (Manheim *et al*., 2012, pp. 351, 360). The three stages of coding have been done manually, without the usage of specific software. The whole process has been recorded in different documents that are being published in a separate codebook for this study.

3.4.Limitations

When using the methods aforementioned, certain limitations were encountered. Firstly, in the communication process, several organisations from the health sector were unwilling to participate in the study as it was first aimed. Therefore, the sectors of the study were reduced from four to three (digital, transportation, and public administration). Secondly, the interviews were online which can impede the contextual information that can be important to interpret the interview data at first, but after the getting-to-know meetings, this was eliminated to a certain extent. Thirdly, we complement the information already published with different interpretations of the interview data. In addition, quantifying or coding interview data can be useful means of providing a sense of the entire interview land space (Mosley, 2013, p. 24). Some might argue certain concerns regarding the way the coding is made due to certain biases from the interviewer when selecting the information and discarding other information, therefore this research work by publicly sharing all the data set and codebook allows for others to reevaluate the scholar's coding and modeling decisions (Mosley, 2013, p. 24). However, this might conflict with ethical considerations for confidentiality purposes. To avoid certain biases, the codebook of the three cycles of coding is being published, so the reliability and validity of the data are fulfilled.

Chapter 4. Literature review

This current section reviews the state of research and arguments around the chosen research spectrum from several strands of literature focusing on legal and governance disciplines, while focusing on the security studies such as cybersecurity and cybersecurity risk-management-related literature.

4.1.The governance of cybersecurity risk-management

Before delving into the literature, it is relevant to follow a general-to-specific approach when analysing the strands of literature on cybersecurity risk-management governance in the EU and the legal framework for it to take place.

Firstly, some scholars argue that countries with public governance ecosystems are more likely to use European institutions to advance their industry-related preferences, while countries with predominantly private governance ecosystems are more likely to emphasise other preferences, rather than industry-specific benefits, in their interaction with European institutions (Calcara & Marchetti, 2022, p. 1243). This framework allows to identify of three analytical properties through which it is possible to compare different state-industry relations: i) protection by the government; ii) cooperation between the public and private sector's elite network; and iii) the level of autonomy from the industry's influence (Calcara & Marchetti, 2022, p. 1255). Also, these scholars stress the US-China competition over power and the consequent creation of two different spheres of technology, each with its products and standards, arguing that this may lead to Europe's risk of being pulled to one side or the other, rather than creating its technological sphere (Calcara & Marchetti, 2022, p. 1257). Overall, this translates to legal measures that could potentially be highly influenced by this tension, with overregulation or under regulation from the EU's side. Therefore, the EU must develop its cybersecurity policy to be able to implement tailor-made measures for the diversity of Member States. However, some scholars, politicians, and business owners might consider that the EU tends to overregulate cyberspace and the path to follow should be more similar to the US approach, e.g., less regulation (Second NISDUC Conference, 2023). Therefore, how this needs to be achieved is an open debate and it is still ongoing, which allows for this research to take place and to ultimately assess to what extent the cybersecurity approach in the Netherlands has been successful.

Other studies focus on the debate regarding the cyber-domain private ownership in which state-industry cooperation is essential to ensure cybersecurity, e.g., an attack on industrial software owned by a private company may have also important consequences for national security, considering the critical infrastructure in some countries is privately owned (Calcara & Marchetti, 2022, p.1238-1239). The regulatory 'hands-off' governance approach reflects the development of digital technologies as fully in the hands of the private sector (Cavelty & Smeets, 2023, p. 1332), for which the question of who has and has not the authority in cybersecurity issues becomes a central issue for democratic politics (Cavelty & Smeets, 2023, p. 1347). Adding to this, other studies stipulate the governance in cyber by trying to better understand the cybersecurity provision by states worldwide in response to global transformations. Showing that governments delegate authority but maintain elements of hierarchical control when they respond to threatening attacks, e.g., information-sharing schemes (Weiss & Jankauskas, 2018, p. 260).

Cybersecurity knows no borders, cybersecurity issues have impacts online but also in the physical domain, e.g., communication processes, transportation, critical infrastructure, or supply chain. For this, the governance of cybersecurity risk-management in a country is key. This is the case because the more cross-border and cross-sectoral cooperation and collaboration, the more a country and consequently other countries are better prepared in cyberspace. Therefore, the more all of the countries are prepared and the more information schemes are in place, the better. Furthermore, a good risk-assessment and effective risk-management are crucial to avoid or at least reduce the risk of this happening shortly. However, how can this be analysed in practice is the main key question for this research. Consequently, this study will depict the practicalities of how the governance of cybersecurity risk-management works in practice at the national level through the case study of the Netherlands to analyse how the legal, political, and IT spheres are aligned to make cybersecurity risk-management measures effective.

4.2.The EU as an actor in cybersecurity and digital policies

In the past ten years, the EU has been developed as a cybersecurity actor. This is the case because cybersecurity has gained over time global importance rather than sector-specific or IT-specific relevance. The publication of the first cybersecurity strategy in 2013 is key in this regard. Therefore, the amount of actors involved has increased over

time and the EU is part and parcel of this complex amalgam of actors, national infrastructures, and locations. Broadly speaking, a lot of actors shape the cybersecurity requirements internationally, at the EU level, and nationally. Therefore, cybersecurity awareness is key, as also knowing and trusting the actors involved in the process. For instance, actors from the local, regional, national, and international levels, also multinationals with a lot of power in the digital domain in cross-border activities, public and private organisations, citizens, IT developers, hackers/hacktivists, and so on. Other factors to take into consideration are the legal frameworks at the EU level and at the international level, which overlap. For instance, in the cases of multinationals based in different countries, this can have ethical consequences.

Cavelty and Smeets (2023, p. 1336) stipulate cybersecurity as a public policy issue that has been defined at the EU level through different directives and regulations that pinpoint the importance of looking for better standards and protections for EU citizens. For this purpose, the evolution of the European Union Agency for Cybersecurity (ENISA) and cybersecurity policies in the EU to take into consideration since the 1990s, is relevant. More concretely, the publication in 2013 of the first cybersecurity strategy developed a more comprehensive and integrated cybersecurity policy for the EU, being the first approach of the EU in this matter.

It is also important to mention the process of renewal of the EU's strategy and the introduction of new legislative proposals such as NIS and NIS2 Directives. Also, the entry into force of the Cybersecurity Act: Certification and ENISA mandate in 2019; the proposals for Digital Operational Resilience Act (DORA) Regulation, the Critical Entities Resilience Directive (CER) in 2020; the entry into force of the Cybersecurity Competence Centre and Network in 2021; the proposal of the European Cyber Resilience Act (CRA) in 2022; and, finally the proposal of Cyber Solidarity Act and the Cyber Skills Academy in 2023. All of this policy and rulemaking allows for the EU to be an actor in cybersecurity. In 2020, both CER and NIS2 proposals came to fruition, but the main differences between both are that CER tries to impose eleven adopted obligations on products as essential requirements of the union legal market, while the NIS2 is about sectoral operators measures at such (Second NISDUC Conference, 2023a). This will be further analysed in the section *'Legal framework'* below.

Although the EU has developed its role as a cybersecurity actor lately, there are some gaps in the actual EU cybersecurity policy such as a lack of budget for the many technologies existent, e.g., AI, quantum technologies, robotics, cybersecurity, 5G and IoT (Timmers, 2018, p. 380). Consequently, even though the ultimate goal of these legal frameworks is to provide the EU with the specific toolkit to be resilient and ready to tackle cyber-risks and incidents, the resources for the Member States to do that are relevant to take into consideration. Therefore, the duty to ensure that the level of security is needed by both industry and the people are part of the EU institutions' task at the moment (Masters of Digital, 2023). The main common ground regarding this is that intersectoral cooperation, at the EU level and internationally is key for an issue that transcends national borders. Furthermore, resources for this to happen need to be considered and fulfilled with the policies in place at both the EU and national levels.

According to Backman (2022), there are considerable gaps in the understanding of the contents and specifics of the tension between EU cybersecurity ambition and Member State contestation. Therefore, the central point of this study is that the lack of understanding of the dynamics of risk and threat-based security logics in EU cybersecurity policy and practices leaves out an essential perspective to understanding development, change, and resistance in international cybersecurity cooperation. Consequently, this already shows one of the gaps to fill in with this research through the procedural and enforcement effectiveness of cybersecurity risk-management measures in the Netherlands. This is the case because cross-border cooperation and public-private collaboration are something that needs to be done in practice, as well as information-sharing schemes or uniformity of the measures in place. Hence, it is important to analyse how and to what extent this is happening in practice in the case of the Netherlands, not only in the national laws but also in the governmental approaches to the implementation of this EU legislation.

Other studies focus also on the trust process. This process is relevant in cybersecurity because all actors need to trust their counterparts to share information, collaborate and consequently achieve the ultimate goal at the EU level: a high common level of cybersecurity. By trusting the counterparts, procedural and enforcement effectiveness might come as a result, as has been exposed in the '*Theoretical framework'* section. Since the more you trust, the more you share your knowledge and the more you are ready in

terms of risk-management and tackling incidents. These terms have been further discussed in several conferences attended, e.g., Masters of Digital and Second NISDUC. Therefore, trust processes in this specific issue are key according to all the actors involved, e.g., public and private sectors, government, and EU institutions. In this regard, trust has been explained in Chapter 2 as a precondition to the factors of procedural and enforcement effectiveness.

The EU single market, the Member States' preferences, as well as the trust processes within the EU Member States but also with international partners, have an impact when analysing the activities and actions that the EU takes to update cybersecurity policies, which consequently slows down a rapid transformation of the tools to implement the cybersecurity risk-management measures needed.

Overall, the EU is launching different legal frameworks that could allow for more in-depth coverage of the cyberspace domain. However, some scholars, politicians, and practitioners may argue these new legal framework overlap, making it difficult for entities and organisations to know what measures to implement and what procedures to follow (Second NISDUC Conference, 2023). In cybersecurity, the EU is becoming an important actor internationally, but a coherent EU policy might be necessary to tackle the multiple security issues that affect its citizens and Member States. But, according to Carrapico & Barrinha (2017, p. 1267), the EU has often achieved unanimity at the expense of effectiveness, meaning that most of the time the need for unanimity might hamper the wanted effect of the policy or legal framework in the first place because to achieve the high common level of cybersecurity it needs to be accepted by 27 Member States with huge differences in their national cybersecurity policies' resources, actions taken, or even definitions of the same issue, e.g., cybersecurity risk-management.

Overall, the main takeaway is that the EU is becoming a more relevant actor, but its supranational, political, and economic nature impedes or slows the process of an effective assessment of cybersecurity risk-management, since cybersecurity is a rapidly changing environment for which the EU needs to establish common ground because otherwise, each Member State would eventually be operating differently. This research will assess whether this is the case in practice through the Dutch case study.

4.3.The legal framework of risk-management in the EU

As was aforementioned in the section above, CER, NIS, and NIS2 Directives among others have been the different proposals by the EU institutions for the continuum of EU-wide cybersecurity legislation, for critical entities, resilience, and so on. In this regard, the implementation of both CER and NIS2 Directives into Dutch national law has been postponed to autumn 2023 and to enter into force in late 2024. This is the case because this is an extensive and complex process. After all, it has been decided to implement both directives in conjunction (NCSC, 2023a). Therefore, the law is expected to enter into force at the end of 2024, after being debated by the Parliament. Organisations under the scope of the NIS2 Directive will have to comply with the duty of care and duty of notification from both (NCSC, 2023b).

Regarding the NIS Directive, some scholars argue that requires all Member States, key internet enablers, and critical infrastructure operators to ensure a secure and trustworthy digital environment throughout the EU (Cavelty & Smeets, 2023, p. 1339; Markopoulou *et al.,* 2019). The EU sought to implement the NIS Directive through both capacity-driven and regulatory measures (Cavelty & Smeets, 2023, p. 1339). Both the NIS and NIS2 Directives are clear examples of rule-based governance (Cavelty & Smeets, 2023, p. 1341), and the new EU's legislative framework is broadened because more entities are obliged to implement cybersecurity measures (Cavelty & Smeets, 2023, p. 1342). According to other studies, the NIS Directive could be considered a late response to an already exacerbated and well-known problem worldwide for which countries like China and the US have introduced their cybersecurity laws (Carrapico & Barrinha, 2017, p. 1267). Consequently, if the EU wanted to be competitive in the international arena specific legal framework would be needed. As it was aforementioned, since 2016 the EU institutions have come up with proposals, directives, and regulations with this objective in mind, to make the EU a world digital hub. This will be further analysed through the case study of the Netherlands and the implementation of the NIS2 Directive.

However, the NIS Directive does not provide sufficient clarity as regards the scope criteria for OESs or the national competence over digital service providers. This has led to a situation in which certain types of entities are not required to put in place security measures and report incidents (European Parliament, 2022, p.6). Moreover, it was shown that some Member States have implemented certain requirements in different ways,

therefore creating an additional burden for companies operating in more than one Member State. Consequently, the NIS2 Directive tries to improve that by increasing the scope of the Directive and introducing a size-cap rule for determining which entities meet the criteria to quantify as operators of essential services and important entities, which means that all medium-sized and large entities operating within the sectors or provided services covered by the Directive would fall within its scope. Such entities would fall under the jurisdiction of the Member States in which they are established, not of the Member States in which they provide their services (European Parliament, 2022, p.12). Among the sectors taken into account are telecoms, social media platforms, and public administration. It removes the distinction made between OESs and digital DPSs which currently fall into three categories: online marketplaces, search engines, and cloud service providers. It reduces inconsistencies in resilience across the internal market. It establishes a minimum list of administrative sanctions whenever entities breach the rules regarding cybersecurity risk-management or their reporting obligations laid down in the NIS Directive.

Also, improving the level of joint situational awareness and the collective capability to prepare and respond by i) taking measures to increase the level of trust between competent authorities; ii) sharing more information; and, iii) setting rules and procedures in the event of a large-scale incident or crisis. The Directive establishes an EU-Cyber Crises Liaison Organisation Network (EU-CyCLONe) to support the coordinated management of EU-wide cybersecurity incidents, to ensure the regular exchange of information, and to strengthen the role of the NIS Cooperation Group. The NIS Cooperation Group (Directive 2016/1148, article 11; Directive 2022/2555, article 14), together with the Commission and ENISA, would be tasked to carry out a coordinated risk-assessment per sector of critical ICT services, systems, or products including relevant threats and vulnerabilities (European Parliament, 2022, p. 9).

The obligations of both NIS and NIS2 Directives are very similar: i) the duty of care, which requires entities to conduct their risk-assessment based on which they take appropriate measures to safeguard their services; ii) the duty to report, which requires entities to report incidents to the regulator within 24 hours and in the case of a cyber-incident it needs to be reported to the CSIRT (regarding the number of people affected by the disruption, the length of time of the disruption and the financial lossess); and, iii) supervision, which will look at compliance with the obligations of the Directive for those

organisations under the scope of NIS2 (NCSC, 2023c). Moreover, the NIS2 Directive requires Member States to support critical, essential, and key entities in improving their resilience to digital risks. The Directive also requires that critical entities be supported with advice and assistance by a CSIRT. Support from the government can further include information sharing, guidance, and resilience-enhancing tools such as for conducting a risk-assessment (NCSC, 2023c). Among the basic measures that organisations can implement to better protect themselves (NCSC, 2023c) are: i) inventory, and analyse risks; ii) establishing business continuity plans and crisis management protocols; iii) identifying alternative supply chains; iv) raising staff awareness of risks and actions to be taken; and, v) set aside budget and capacity needed to meet the guidelines.

In light of the NIS2 Directive, Member States should promote the use of relevant European and international standards by essential and important entities or the usage of certified ICT products, services, and processes, to demonstrate compliance with cybersecurity risk-management measures (Directive 2022/2555, paragraph 80). It is important to add here some of the international standards that the Directive refers to and that are widely used in practice. The Directive names ISO 30111 and ISO/IEC 29147 to provide guidance on both vulnerability handling and disclosure (Directive 2022/2555, paragraph 58); and stipulates fostering alignments with international standards and existing industry best practices in cybersecurity risk-management (Directive 2022/2555, paragraph 59). First, ISO standards could be about making a product, managing a process, delivering a service, or supplying materials – standards cover a huge range of materials. Among the ISO standards that this study takes into account are: ISO/IEC 27001:2013; ISO/IEC 27005:2018; or ISO 31000: 2018. Secondly, NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework gives, voluntarily, businesses best practices to help them understand, manage, and reduce their cybersecurity risk and protect their networks and data.[7] These are standards used and made by the private sector. However, in practice, each time more and more public administrative bodies are using them.

Likewise, for Member States to ensure effective compliance from the supervisory side, they should ensure that the competent authorities when exercising their supervisory tasks

[7] *Framework for Improving Critical Infrastructure Cybersecurity*, NIST 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

can assess *ex post* the cybersecurity risk-management measures adopted, e.g., documented cybersecurity policies or the submission of information to the supervisory authority (Directive 2022/2555, paragraph 112; article 33(2)(d)).

Although Member States would still be required to adopt a national cybersecurity strategy and to designate one or more national competent authorities to supervise compliance with the Directive; and to designate CSIRTs to handle incident notifications and single points of contact to act as a liaison point with other Member States (European Parliament, 2022, p. 7). The NIS2 takes into account the CER Directive, DORA, and the SPEAR project to ensure consistency and coherence with related EU legislation (European Parliament, 2022, p. 8).

The provisions that are being taken into account in this research, in light of the NIS2 Directive, are the governance and cybersecurity risk-management measures, reporting obligations to a lesser extent, the role of the competent authorities and CSIRTs in the Netherlands, as well as the collaboration and cooperation schemes nationally and at the EU level in all its forms (Directive 2022/2555, articles 1, 3, 20, 21, 31, 32; Directive 2016/1148, articles 8, 9, 10, 11, 14).

Given that the NIS and NIS2 Directives are the first regulatory attempt at the EU level for the protection of information systems and because the Directive aims to regulate a sector under constant reform and development, it has been argued that flexibility in implementation could be beneficial shortly to avoid re-writing the legal frameworks over and over again. However, the debate is still ongoing because allowing Member States both flexibility and time for response could hamper the EU's ultimate goal of the creation of a high common level of cybersecurity. According to Markopoulou *et al*. (2019, p. 7), allowing Member States to adapt to the Directive's provisions to the needs and special characteristics of the undertakings operating within their territory could contribute to more effective assessment and implementation of the measures and requirements suggested in the Directive, such as cybersecurity risk-management measures.

4.3.1. Case: The Netherlands

In the Netherlands, the fact that the implementation of both CER and NIS2 Directives into Dutch national law has been postponed to autumn 2023 has consequences on the actual implementation by the governmental institutions in the Netherlands of the NIS2 Directive transposed into national law, this will make the process slower.
However, the process of transposition of these Directives is still in the making not only in the Netherlands but in other Member States. Therefore, at the moment the stakeholders involved in the process in the Netherlands: governmental institutions (regulatory bodies, sectorial ministries), CSIRTs, CISOs, ISACs, business owners, and legal advisors are figuring out the transposition of this new legal framework into national law. However, the one that is already in place is the Network and Information Security Act or Wbni (2018), which is roughly called the 'NIS1 Directive for the Netherlands'. Below both the national legislation and the national cybersecurity strategy for the Netherlands will be further discussed.

a. National legislation

The Wbni (2018) serves as the guidance document for the Netherlands to implement the NIS Directive within the different sectors. Although the NIS Directive is not the main focus of this research, it is the first attempt of achieving a high common level of network and information systems within the EU (Directive 2016/1148, article 1). However, already a culture of risk-management is mentioned in the preamble of the Directive. Therefore, this section will focus specifically on the risks to properly analyse the issue that is relevant to the scope of this research.

Consequently, the culture of risk-management involving risk-assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices (Directive 2016/1148, paragraph 44). Moreover, according to the Directive, the risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents, and to mitigate their impact (Directive 2016/1148, paragraph 46). The latter is related to the enforcement effectiveness framework further explain in the *'Theoretical framework'* section in which one of the factors is being repellent enough

to cyber-risks and this is exactly it. Meaning that by knowing the organisation's potential risks through the risk analysis, measures can be implemented within the organisations to limit their impact. Although 100% security does not exist, all the measures taken to have higher maturity levels are positive for organisations in the Netherlands. This will be further analysed in Chapter 5 with the empirical findings resulting from the interviews.

However, these measures are not further specified throughout the articles of the Directive. In this regard, the Wbni (2018, article 7.1) stipulated that 'the provider of an essential service and the digital service provider shall take appropriate and proportionate technical and organisational measures to control the risks to the security of their network and information systems'. The measures of the digital service provider shall take into account the following: i) security of systems and facilities; ii) handling of incidents; iii) business continuity management; iv) monitoring, control, and testing; v) compliance with international standards. Moreover, this national law specifies that the vital provider should report to the Ministry about an incident with significant consequences or a breach of the security of network and information systems (Wbni, article 10.1.) for which, the notification of that should be accompanied by the measures taken by the provider to limit the consequences of the incident whenever is possible (Wbni, article 11.e.). It is therefore understood that the measures are tailor-made in the specific case of each sector according to the mandates of the Wbni (2018).

Therefore, already cybersecurity risk-management is being taken into account within the first NIS Directive. However, a list of specifics is missing for which the NIS2 Directive goes more in-depth in this issue, more concretely cybersecurity risk-management framework and measures. Whether these will be implemented in the Netherlands is still to be seen shortly and once the Directive is transposed into national law because, at the moment, entities are taking into consideration the NIS mandates. Consequently, this research comes up with policy recommendations to shed light on the topic of cybersecurity risk-management measures in practice and the transposition of the EU legal framework in national law. Further analysis is provided in Chapters 6 and 7 of this research work.

b. National Cybersecurity Strategy 2022-2028

The National Cybersecurity Strategy 2022-2028 is the latest cybersecurity strategy policy implemented by the Dutch government. It is formed by four pillars and five main priorities. Among its four pillars are: i) cyber resilience of the government, businesses, and civil society organisations; ii) secure and innovative digital products and services; iii) countering cyber-threats posed by states and criminals; iv) cybersecurity labour market, education, and cyber resilience of the public. Whereas, among its priorities are: i) be more aware of cyber-threats so that we know and understand them; ii) ensure sufficient cyber expertise is available on the labour market so that we can meet the challenges we face; iii) be aware of and understand risks and threats; iv) legislation to ensure that frameworks are clear and verifiable; and, v) review of national cybersecurity system to ensure effective and efficient use of cyber capabilities.

According to the strategy, a single phishing email or lost password can have a huge impact. This is part of the responsibility for risk-management for an entire ecosystem, including critical sectors and processes, lies with the least digitally mature participants, which according to the strategy are: individuals, small businesses, and local authorities (NCTV, 2022, p. 7). Regarding the pre-implementation phase of this strategy, it is accompanied by an action plan that could be adjusted regarding the changes in the interests at stake, the threat, resilience levels, or other political/administrative requirements (NCTV, 2022, 47).

Furthermore, this strategy coordinates an integrated risk-management within and between the organisational, sectoral, and national levels, which is still in its infancy (NCTV, 2022, p. 13). According to the strategy, setting up a sound risk-management system is key in organisations, therefore the specific decisions on this process need to be taken by a director or senior management board within the organisation (NCTV, 2022, p. 27).

Under legislation such as the NIS2 and/or sectoral legislation for that matter, regulated organisations are currently obliged to account for their cybersecurity measures to supervisory authorities, which have various instruments to encourage organisatons under their supervision to increase and maintain their resilience, supervisory authorities also have good oversight of the actual resilience of organisations and sectors (NCTV, 2022,

p. 27). Among some sub-aims highlighted by this strategy, there is that organisations also focus their risk-management on cybersecurity risks, and increase transparency in this regard (NCTV, 2022, p. 28). Consequently, certain topics covered in the literature and the empirical findings from the interviews are also stipulated in this strategy. Concepts such as tailor-made approaches for the sectors, trust, and information-sharing schemes appear throughout the strategy. Also, increasing awareness and resources on cybersecurity, so the organisations reach a specific maturity level. Moreover, consistency in terminology nationally on the resilience of critical entities (NCTV, 2022, p. 26), as well as harmonisation on the implementation of European and national legislation in the Netherlands are aimed for (NCTV, 2022, p. 27).

Overall, collaboration, information sharing, harmonisation, and trust seem the main drivers of this strategy which adds up to what has been discussed in the *'Theoretical framework'* section of this study.

4.4.The risk-management in practice

When assessing risks and developing risk-management frameworks, public and private partnerships are key to the process in practice. This is the case for two main reasons. Firstly, information sharing allows for better understanding of the nuances of the digital world. Secondly, the private sector has more resources than the public sector. This allows for other ways to approach the same problem, and it also comes with more standards needed to fulfill. Whereas the hard enactment of policies remains feasible, softer forms such as public-private partnerships are more complementary to address this challenge than hierarchical top-down impositions, and several reasons explain this. Firstly, implementation depends on the willingness of third parties to comply with new rules, which is arguably enhanced when they become integral part of the initial decision-making setting (Weiss & Jankauskas, 2018, p. 265). Secondly, the private and public partnerships are relevant in the process because the private sector has the resources and standards in place that are considered as the main thing to take into consideration and then the public sector follows upon these approaches.

There are government bodies such as NIST, the worldwide Federation of national standard bodies such as ISO, agencies such as ENISA and independent organisations such as OWASP continuously reporting on the security-relevant aspects of cyberspace

(Refsdal *et al.*, 2015, p. 121). Therefore, cross-border cooperation in cybersecurity risk-management activities is relevant for an effective outcome in countries such as the Netherlands. This study wants to zoom in on this cooperation and collaboration in practice (and in all its forms: national, cross-border, public-private) to assess the procedural and enforcement effectiveness of cybersecurity risk-management measures since these factors are relevant and have been explained in the *'Theoretical framework'* section of this study.

Both the public and private sectors are following in practice standards such as ISO or NIST as it was further discussed in the Second NISDUC Conference attended in April. According to the IJenV (2022, p. 9), within risk-management, an ISO 27001 certification contributes to the IT and OT governance of vital service providers. It shows that measures are continuously monitored and further improved where necessary. With these certifications, also come the inspection activities that show that vital service providers respond quickly to vulnerabilities. However, being certified by these standards does not necessarily mean being 100% secure (Weber, 2023; Second NISDUC Conference, 2023).

In this regard, it is important to mention that if complying with standards such as ISO or NIST does not improve risk-management, then those standards and regulations need to change (Hubbard & Seiersen, 2016, p.56). Therefore, some scholars argue that when after using cybersecurity risk-analysis, an organisation cannot perceive any improvement whatsoever, then that consists of a high risk in cybersecurity and improving risk assessment will be the most important risk-management priority for that organisation in particular (Hubbard & Seiersen, 2016, p.55-56). According to the authors, the importance of cybersecurity risk-assessment means that we must continue to seek improvements in our methods (Hubbard & Seiersen, 2016, p.77). Consequently, the risk-management process does not only start when risks have been identified but also during the whole process of evaluation, mitigation, and follow-up measures. Then, supervisory activities are key in the process of risk-management in a Member State such as the Netherlands. In this regard, supervision allows to show the entities the need of compliance for them to be aware that risk-based/proactive approach without any sound foundation comes into an endless discussion (Second NISDUC Conference, 2023b).

According to Refsdal *et al* (2015), it is important to achieve a common agreement on and mutual understanding of how risks should be managed among all relevant stakeholders.

With this in mind, the main purposes of the monitoring and review processes are as follows: i) ensure that controls are effective and efficient; ii) obtain further information to improve risk-assessment; iii) analyse and learn lessons from incidents, changes, trends, successes, and failures; iv) detect changes; and, v) identify emerging risks (Refsdal *et al.*, 2015, p. 22). Also, since cyberspace is continuously evolving, the process of cybersecurity risk-management needs to be dynamic and needs to be computerised, because otherwise, it will not be possible to react in time. This includes how risk-assessments are planned and conducted, to what extent measures and controls are implemented, and how information is obtained and communicated (Refsdal *et al.*, 2015, p. 46).

An important challenge faced by governments in general and the Dutch government in particular is the management of national infrastructure security. Information technology infrastructure has been recognised as one of the critical elements of this national infrastructure (Ogut *et al.*, 2011, p. 507). This is the case because we are highly dependent on information systems; moreover how wires and communication systems are settled has a huge impact on whether the security measures and standards are fulfilled nationally. The national information technology infrastructure includes firms of different sizes, information technology assets, and capabilities. It might be the case that smaller firms free-ride on larger firms in managing their security. This may mean that the optimal strategy to follow could be to use different sizes, information technology assets, and capabilities (Ogut *et al.*, 2011, p. 508). This study will also zoom in on this issue specifically to check if this happens in practice in the Netherlands as well as to check what standards and practices are in place in practice in the digital, transport, and public administration sectors.

Other studies zoom in on the companies' size and to what extent they are affected by insider threats. More concretely, how these threats affect small and medium-sized companies (SMEs) in the Netherlands, due to be an understudied population in the country (Moneva & Leukfeldt, 2023). The case of SMEs is interesting because even though it is not a population that is covered under the scope of the NIS2 Directive, the resources of the companies make a change when dealing with reporting schemes. Although it seems that, in general, larger companies report more incidents, they also have

more resources and therefore probably better detection tools and reporting mechanisms (Moneva & Leukfeldt, 2023, p. 2).

According to this study, most SMEs apply basic measures in terms of cybersecurity rules and controls but as with risk-management measures, the cybersecurity policies of most SMEs do not cover many important aspects (Moneva & Leukfeldt, 2023, p. 16). Other papers' findings suggest that a certain level of cybersecurity infrastructure is needed to adequately detect incidents and further investments in cybersecurity measures help to prevent incidents in companies and/or entities (Dinkova *et al.*, 2020, p. 23). There is a differentiation in the approach towards SMEs' actions regarding cybersecurity in this regard, since some scholars argue that SMEs are insufficiently aware of cyber-risks and to invest too little in prevention; while large firms are exposed to more outside threats due to a higher visibility and a more intense usage of ICT systems (Dinkova *et al.*, 2020, pp. 2-3).

However, other scholars explain that factors such as the size of the company, its business, and its dependence on IT systems can influence people's persceptions when showing concerns about cybersecurity within the organisation they are part of (Moneva & Leukfeldt, 2023, p. 20). Therefore, they focus on the human factor when assessing SMEs actions towards more cybersecure ICT systems. Consequently, in practice, either if you are an SME or a larger company, cybersecurity risk-management framework needs to be in place, for which information-sharing schemes, trust, and harmonisation might be key. Therefore, this research has the purpose to zoom in to check whether or not this is happening and whether or not this is the approach to follow in the Netherlands. Even though the main focus of this study is not about SMEs per se, the approach of the private-public partnerships is taken into consideration in this research.

Overall, this section has depicted the main strands of literature and the main debates that are ongoing regarding cybersecurity risk-managament framework in EU Member States. The main findings are threefold. Firstly, the debate regarding compliance and risk-based approach in cybersecurity is still ongoing in practice in the Netherlands, in which supervisory activities are seen as key in conjunction with certifications/standards. Secondly, the EU is an important player in cybersecurity, but its supranational nature difficult the agreements between Member States and can lead to overlap in the legislation. Thirdly, the case of the Netherlands has been understudied in the literature which allows

for this research to take place, while the resources of companies in the Netherlands might have an impact on their approach to cybersecurity risk-management.

Chapter 5. Results and discussion

In this section, the main objective is to present the results from the main research pillars and designs used in this interdisciplinary research. These research types are perspectives from the theoretical framework, literature review, and interviews. The main idea in this section is to compile all the data gathered both during the literature review and coding of the interviews, and several conferences attended, while assessing all this data from the perspectives of the theoretical framework. This is the case to be able to analyse and assess the data and answer the main research question and sub-research questions.

In the following section, the state-of-art of cybersecurity risk-managament in the Dutch critical infrastructure as well as the debates regarding compliance or risk-driven approaches will be further analysed through the information provided by the interviewees. Their responses have been fully anonimised.

The next sections will analyse more in-depth the sub-questions of this research in the following order: i) cybersecurity risk-management; ii) cybersecurity risk-management measures; iii) procedural effectiveness – factors; and, iv) enforcement effectiveness – factors. The main objective is to be able to analyse the main research questions of this research regarding the implementation of the NIS2 Directive in the Netherlands.

5.1.Cybersecurity risk-management

Article 6 of the NIS2 Directive specifies the definitions of the different concepts that appear throughout the Directive, e.g., ICT systems, incidents, threats, and so on. However, the concept of cybersecurity risk-management does not appear, even though it is being used throughout the Directive consistently. There are similar concepts that are being defined such as risks or incidents, but no definition per se of cybersecurity risk-management and what it entails. First of all, it seems this definition needs to be shaped by each Member State due to the open nature of a Directive in EU law. Secondly, each Member State has different levels of maturity which could imply different conceptualisations of the same topic or different resources used. Thirdly, within the governmental institutions, there can be certain overlaps within the definitions, thus different documentation and procedures within the same government. Lastly, the lack of

a common definition might imply misunderstandings. Consequently, the ultimate goal of the directive: a high common level of cybersecurity would be hampered.

In the following section, topics and articles of the NIS2 Directive as well as certain policy reports that have been shared during the interviews are going to be explained, while analysing the empirical findings and juxtaposing them with the findings of the literature review and the theoretical framework.

When conducting the interviews, one question was regarding the definition of the concept 'cybersecurity risk-management framework' (see Appendix D). Through the interviews conducted I found out there is no consistency regarding the definition of cybersecurity risk-managament, meaning that each respondent gave slightly different approaches to a common issue. Now, some specific examples of the respondents' answers will be provided to give light on this topic. Firstly, *risks are the weaknesses that your system has that can make you being hacked and the potential impact that those hacks might have* (respondent 2). However, the nature of the company, meaning public or private organisation has an impact on how important is data theft, therefore what cybersecurity risk-management means, and the measures that need to be taken into consideration depending on a case-by-case basis, therefore a tailor-made approach is needed when it comes to cybersecurity matters according to this respondent. This tailor-made approach has been a common agreement among respondents since a case-by-case basis seems to be needed for each sector regarding cybersecurity risk-management. View shared by respondent 4 as well. Therefore, cybersecurity risk-management is defined slightly differently depending on whom you are talking to and the sector they are part of. However, respondent 8 was skeptical of this tailor-made approach for each sector.

Secondly, for other interviewees, the definition of cybersecurity risk-management starts with the definition set in paragraph two of the NIS Directive: 'the magnitude, frequency, and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence, and cause major damage to the economy of the Union.' It was also discussed that *the management of risks is*

contradicting in nature, since when concepts such as 'cyber hygiene' appear, it is difficult to understand what they entail, therefore there is no clear meaning or procedure to follow to fulfill this concept (respondent 3).

Thirdly, another respondent stipulated that the definition of cybersecurity risk-management is still under debate because *the wording you choose and how you interpret the different layers such as technical measures, operational measures, organisational measures stipulate the control objectives your organisation takes into account and these might differ between entities* (respondent 1). All of this needs to be in connection with the governance set and consequently, more information security management or risk-management processes for companies from an organisational perspective to stipulate the specific measures, and after this process is done you get into the actual measures. Overall, the interview subjects said that different entities are to a certain extent allowed to *choose their own definition when it comes to cybersecurity risk-management, but that best practices such as ISO 27005 were part of the risk-management approach for these entities* (respondent 1). Therefore, organisations have a risk analysis in place and certain maturity levels developed, but supervisory authorities' activities need to be fulfilled to reach the level of cybersecurity aimed at with the NIS2 Directive.

Moreover, according to respondent 4 the main definition of cybersecurity risk-management that his organisation follows is the one provided by the NCSC (2018, p. 9): 'Cybersecurity is the entirety of measures to prevent damage due to disruption, failure and misuse of ICT and if damage does occur to repair it.' However, he specified that since the *NIS2 Directive is still to be transposed into national law, his organisation is developing its handbook in which all these definitions may be further covered*. And that they *take a look into standards such as NIST or ISO* (respondent 4).

In general, the main point taken from all the interviews conducted is to stay near the wording of the Directive even though an exact definition of the term does not appear in Article 6. But other terms are being taken into account, such as risks or incidents. In this line, one of the respondents said that risk-management entails '*basically, all measures that would enable a cybersecurity attack from happening or limiting its impact'* (respondent 5). Also, another of the respondents stipulates that it *is the management of the risk*, therefore *it is about managing the potential loss or disruption caused by an*

incident, also the respondent's organisation is '*alligned with the ISO definition as well as the measures needed to manage the cybersecurity risk'* in the first place (respondent 6).

Therefore, it seems from the respondents' answers that the cybersecurity risk-management should be formed by technical, operational, organisational measures, and the ones stipulated in article 21.2 (a-f) NIS2 Directive can serve as a basis for all organisations. At least this is seen as the first step to follow.

Furthermore, according to respondent 7, his organisation was following the Directive's mandates, the definition in the Netherlands was based on the lower-level national decree (Bbni, 2023) as well as the Wbni 2018. In both, the main takeaways are that 'the provider of essential service and the digital service provider shall take appropriate and proportionate, technical, and organisational measures to control the risks to the security of their network and information systems. Given the state-of-the-art, the measures shall ensure a level of security appropriate to the risks encountered (Wbni 2018, article 7(1)).' On the other hand, according to Bbni (2023, article 9.3), 'the provider has layered a security strategy based on the risks encountered from the risk analysis and according to this, the government agencies assesses whether based on the given state-of-the-art, additional measures are necessary to reduce the identified risks.' Therefore, this respondent aligns with the aforementioned: the cybersecurity risk-management framework should be based on technical, operational and organisational measures.

Finally, another respondent specified that there is no definition written down in particular but the interview subject's organisation has a risk-management department that stipulates risks such as business continuity, safety, financial risks, and environmental risks and for each of their Information Security Management Systems (ISMS)[8] map those risks. Therefore, they are doing a risk-assessment on how the system is related to those risks. Then the organisation gets a risk profile of each of their information security and based on that they determine the measures to take (respondent 8). The interviewee also said that *we want to become better in cyber, so we are not externally driven by NIST or ISO. Now, we have to oblige and comply more to those frameworks/standards. We are trying to find*

[8] A set of policies and procedures for systematically managing an organisation's sensitive data. The goal of this set of policies is to minimise risk and ensure business continuity by proactively limiting the impact of a security breach (Yasar, 2022). The ISMS can be set up as explained in ISO 27001.

a middle ground *between managing the risk and enabling the* organisation *in their digitalisation* (respondent 8).

Overall, the definition of cybersecurity risk-management still needs to be shaped, but the main ideas taken by the interviews are: risk-management entails the whole process of different layers such as technical measures, operational measures, organisational measures that stipulate the control objectives the organisation takes into account and these might differ among entities but they are laid down in the Directive's mandates. Therefore, the risk-management approach is tailor-made, but in principle risk-management serves to prevent damage due to disruption, failure, and misuse of ICT systems and if damage does occur, to be able to repair it. Moreover, ISO standards serve as a basis for this definition for all organisations notwithstanding their nature.

Acording to the Cyber Security Assessment Netherlands 2022 (CSAN, 2022), risk-management at national level is still in its infancy. This is the case due to various reasons. Firstly, in the development towards a mature approach of risk-management at organisational, sectoral and national level, information-sharing schemes regarding risk-analyses should be done. Secondly, concepts, methods and techniques are primarily tailored to the level of individual organisations even though attackers can operate from different countries, use the infrastructure of different countries, create victims in many countries and do not comply with legislation and regulations (CSAN, 2022, pp. 28-29). Consequently, attending to what has been discussed in the literature review and the empirical findings of this study, the takeaway is twofold. Firstly, the priority of cybersecurity risk-management in an organisation is to seek improvements on the approach used, because risks are different in nature and cybersecurity knows no borders. Secondly, risk-management does not only start when risks have been identified but also during the whole process of evaluation, mitigation, and future assessment. Overall, a main empirical finding is that there is no 100% security, therefore updated cybersecurity risk-management needs to be fulfilled at all times.
The NIS2 Directive by not defining the term cybersecurity risk-management framework leaves leeway to Member States on their approach, which complicates a common idea of what needs to be done in practice and creates an ongoing debate on definitions that need to be stipulated since the beginning if the idea is to implement the Directive in the national system of the Netherlands. Therefore, preconditions of risk-based approach, compliance,

trustworthy networks, or harmonisation are key when assessing both procedural and enforcement effectiveness at the national level by following the Directive's mandates decided at the EU level.

5.2.Cybersecurity risk-management measures

Article 6 of the NIS2 Directive specifies the definitions of the different concepts that appear throughout the Directive, e.g., ICT systems, incidents, threats, and so on. More concretely, the cybersecurity risk-management measures are named throughout the Directive multiple times. However, there is no strict definition of them in Article 6. On Article 21 some measures are stipulated as it was showcased in the subsection '*Terminology'*. However, these are quite general and consequently, each Member State might come up with its own definition following these commonly agreed standards at the EU level. Thus, some of the main ideas shared by the respondents will be further discussed hereafter.

Through the interviews, the definition of cybersecurity risk-management measures was non-consistent. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic. Firstly, according to respondent 4, these measures are based on the risk-assessment of economic impact, e.g., the cost of flights and the impact on society, to prioritise the means of inspection. Within his organisation, they take into account the Inspection-wide Risk Analysis (IBRA). Therefore, according to the IBRA report (2022, p.12), the calculated damage is divided into four different subcategories: i) physical damage, ii) damage to health, iii) environmental damage, and, iv) economic damage. IBRA method is based on multi-year insights and describes the social risks as objectively as possible and this is the report on which the ILT bases its deployment of people and resources (IBRA, 2022, p. 21). Therefore, the measures taken into consideration are tailor-made to the specific risks encountered in the specific sector.

Secondly, other respondents stipulated the technical and organisational measures mentioned in the Directive (respondents 1 and 6). *The orgnanisational measures offer a control framework for technical measures to keep them up-to-date as well as suitable for the circumstances in* which *they are used in* (respondent 1). With the NIS2 Directive, it is still under debate, but previously *we looked at detection monitoring on logging because*

detecting incidents rapidly is very important; also business continuity management since you cannot prevent all incidents from happening (respondent 1). The interview subject argued that *sometimes it is not possible to take a measure in practice but you can take other measures like compensating measures via different routes, to address the risk*; but that ultimately it is the individual's responsibility *to take the measures to manage the risks* (respondent 1).
For other respondents, *cybersecurity risk-management measures are usually technical, following standards such as ISO, but it is on a case-by-case basis* (respondent 2). This respondent argued that depending on whether your information is of public knowledge, *you might approach your cybersecurity differently* (respondent 2). However, when referring to the ISMS, the respondent said it was confidential.

Thirdly, other respondents stipulated that the main driver of the law is the National Coordinator for Counterterrorism and Security by the Ministry of Justice and Security (NCTV). The interview subject referred to the CSAN (2022, p.11) report when being asked about the definition of these measures. In this report, cybersecurity is the 'set of measures to reduce relevant risks to an acceptable level. The measures may be aimed at preventing cyber incidents and, once they have occurred, detecting them, limiting damage, and making recovery easier.' According to this report, an acceptable level is the result of a risk assessment. Consequently, according to respondent 3, *the definition follows the NIS2 Directive definition. However, some words are still not so understandable such as cyber hygiene.* But, according to this respondent, once the transposition to national law occurs, all these questions will fall into place. The respondent meant that is up to the national systems to make these definitions more understandable at the national level. In this line respondent 5 argued the same.
Meaning that *the Directive lays down the minimum that needs to be performed, e.g., incident handling, number of reports to fill in. But the specifics of that are laid down by the national authority, the Dutch government in this case (respondent 5),* because the basis is to establish general awareness. By then, the government will explain what that means to actually have the definion. Adding to this idea, respondent 7 also mentioned the room for interpretation of the NIS2 Directive. He focused on the idea of security requirements and duty of care. *In the Netherlands the lower level law clarifies the security requirements that were not clarified in the NIS Directive or that were rather abstract*. Also, saying that with the lower administrative act there is room for sectoral clarifications

as well (respondent 7). Therefore, the NIS2 Directive sets the basis and is then up to the national governments to stipulate the specificities regarding the definitions of the measures.

Finally, according to another respondent, the organisation has its own information security policy within the organisation*, a high-level policy that establishes the risk-appetite, a policy about identity and access management, a policy about password strength or standards, a policy on how to deal with encryption, and we have a standard on which encryption mechanisms are allowed or not allowed*. *We translated a standard of good practice ISO 27001 plus our* professional *experience* in *our* field. According to this respondent *measures are identity access management, password policies, screening of personal employees or patching vulnerability management, and contracts* (respondent 8).

Therefore, a clear definition of measures is lacking at the moment. But, these measures need to be technical, operational, and organisational, the article 21.2 serve as a basis, and then is up to Member States to develop their national legislation by 2024 and, after that, each sector can delve into more sector-specific clarifications, e.g., tailor-made measures, types of training, risks encountered, standards, etc.
Moreover, supervisory activities are key in the process of risk-management in the Netherlands, since supervision shows the entities the need to take the necessary approaches to reduce risks (Second NISDUC Conference, 2023b).

In the Netherlands, the NCSC has created a guide of cybersecurity measures to make the process simpler for organisations and entities under the scope of the Directive, which is as follows: i) install updates; ii) ensure that each application and system generates sufficient log information; iii) implement multi-factor authentication; iv) control who has access to your data and services; v) segment networks; vi) check with devices and services can be accessed from the Internet and protect them; vii) encrypt storage media containing sensitive business information; and, viii) back-up and test your systems regularly (NCSC, 2021). Although these are measures to be taken by organisations, these organisations need to carry their own risk analysis, since each organisation is unique and can be that a certain organisation requires a tailor-made approach since both threats and interests of the organisation needs protection can change (NCSC, 2021, p. 5). Also, the focus is on IT

and OT devices to effectively proceed and enforce these measures, for which a cybersecurity management within the entity/organisation is needed (NCSC, 2021, p. 4). Moreover, other basic measures to better protect organisations from risk and damage from cyber-attacks are: i) inventory and analyse risks; ii) establishing business continuity plans and crisis management protocols; iii) identifying alternative supply chains; iv) raising staff awareness of risks and actions to be taken; and, v) set aside budget and capacity needed to meet the guidelines (NCSC, 2021).

Overall, there is a common ground in the findings of the interviews conducted regarding the cybersecurity risk-management measures: i) technical measures, ii) operational measures, iii) organisational measures, and iii) ISO and NIST standards serving as a basis. Also, an empirical finding is that there is a lot of room for interpretation due to the NIS2 Directive nationally. Therefore, once the NIS2 Directive is transposed into national law, the supervisory authorities in the Netherlands might stipulate specific measures for each sector. Consequently, a tailor-made approach is used when dealing with this, because each sector has different risks and incidents to take into account. Nonetheless, one of the respondents expressed skepticism regarding sector-specific definitions of cybersecurity risk-management and its measures. The respondent argued that all the measures outlined in NIS2 Directive are rather basic, rendering specifications unnecessary. It is worth noting that the measures considered at the moment are related to the specifics of the NIS Directive and, once the Netherlands transposes the NIS2 Directive into national law, the measures outlined in the NIS2 Directive will be taken into account.
Consequently, the extent to which the NIS2 Directive is taken up in the Netherlands is to debate, because it has been discussed in some interviews conducted that the work from Brussels regarding the NIS2 is completed and that now every Member State will describe the specifics regarding both the cybersecurity risk-managament framework and its measures.

In the Netherlands, the competent authorities take on the definitions stipulated in the EU Directives, but standards such as ISO or NIST are broadly used to be relevant as it was stipulated by respondent 6. In the end, the Directive takes time to be implemented, the process is ongoing and the governmental institutions, organisations, and entities need to follow an approach. Of course, security is always in the making, there is always something to change, therefore being updated and easily adaptable is a must. However, it

seems that the process of digitalisation goes rather quickly, but the legislation lacks rather behind this process. Moreover, the legislation needs to be as broad as possible, because otherwise a lot of specifications need to be made. At the same time, the fact that it is a Directive means that all Member States follow the measures, but some Member States had these measures in place already and others are lagging behind due to a lack of resources and/or maturity levels.

5.3.Procedural and enforcement effectiveness in practice

In this section, the concepts defined previously in the *'Theoretical framework'* section are going to be further analysed through the main findings from the interviews conducted as well as some reports on the topics discussed during the interviews. Because, during the interviewing process, certain questions were asked to measure the factors identified as procedural and enforcement effectiveness respectively.

In the following sections, these factors will be further analysed taking into consideration the data gathered in the interview process. In this regard, the interview information has been fully anonymised due to interviewees' preferences.

5.3.1. Procedural effectiveness – factors

This section will provide a detailed explanation of the primary findings pertaining to each factor included in the *procedural effectiveness* theoretical framework of this study, as outlined in Table 1 above. Additionally, the preconditions necessary for establishing these factors initially, as presented in Table 2 above, will be elaborated upon.

a. Information sharing (nationally)

Information sharing is understood as the process of providing the immediate close network with information regarding incidents or risks, and information on ISMS or best practices. Moreover, it is considered in here the duty to report by entities, therefore sharing the information of an imminent attack or an attack that has happened can be driven by two types of scenarios: i) following the threshold stipulated by law; or ii) on a voluntary basis. The main finding has been that information sharing is a result that organisations in the Netherlands want to achieve, but that often transparency issues arise,

making the information not easily accessible. Moreover, it has been found that NCSC is the main 'information sharer' in the Netherlands. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic. Firstly, one respondent said that *NCSC is playing a supportive role,* they provide the entities with the latest information on threat intelligence, guidance on security measures, and/or instant response. So NCSC is facilitating both *entities and the competent authorities with the general information of what is going on in cybersecurity* (respondent 1). Another respondent also stipulated that *information sharing is done by NCSC, e.g., about risk management, news of any kind, everything that is important regarding cyber* (respondent 4). Moreover, this respondent stipulated that there is within the Netherlands, the *Digital Trust Centre (DTC) in which SMEs and other companies create an information-sharing scheme and they can be up-to-date.* He said that within the maritime *sector they share the information here* because the DTC network is a trustworthy network with which people feel encouraged to share the information with organisations alike. Therefore, one main finding is that information sharing and trust are correlated for this respondent. Therefore, the general principle of trust or precondition as exposed in Chapter 2, comes to the core when dealing with information sharing in the Netherlands.

One finding that has been quite recurrent in the interviews has been the relevance of trust and compliance regarding the information-sharing schemes at the national level. Entities have according to the NIS2 Directive the duty of report, therefore *if the entity has actually had an incident* that *they have to report* to the competent authorities *there are specific thresholds for companies in which they have to report,* according to the NIS2 (respondent 1). This is understood in this study as part of the information sharing, so by sharing this information the entities are sharing their specific situation. However, this implies that the moment the organisations are not reaching this threshold imposed by law, might be that they would not share the information because of not being mandatory. Therefore, it might be the case that the levels of trust between entities and governmental institutions are low and entities comply with the thresholds imposed by law, but not on a voluntary basis.

In addition, the information-sharing process has been related to trust levels, meaning that government *agencies are trusted to handle that information and also have clearances. It is really about the expectations of the entities on where information will end up, with whom it will be shared, and for what purpose* (respondent 1). Moreover, in this regard,

one respondent said the following: *I noticed we talked about sharing specific information with other organisations, and that resulted in a gloved-up session. They were less willing to talk to us because they were afraid that we would actually send specific information to another organisation* (respondent 1). This respondent emphasised that it is all about the trust within the system and the entities. Regarding trust, the respondent also added that this trust is needed between the organisations, because then when *you provide them with information, they will not act upon it in a way that is harmful to the whole system of parties of the societal purpose you want to achieve. That is always the discussion because the different* entities *and governmental authorities are trusted with the information* (respondent 1). Consequently, one main finding so far is that trust and information sharing are interrelated and that both might allow the system to be resilient and ready. But, trust comes as a general principle or precondition for information sharing to happen in practice.

In line with the relevance of a trustworthy network when dealing with information sharing, another respondent said that *with NIS one, it was still feasible to focus on the personal relationship, and a lot of voluntary notifications and information sharing. That information is more valuable than really formal notification* (respondent 7). But this respondent said that with the scope broadening this might be rather difficult. The main point taken is that if the process is too formal, the involvement of a lot of actors is at stake and therefore it makes the process a bit slower, meaning that *you get in sort of a different kind of relationship when it is really getting formal. This* is *why all the more informal contacts are also really valuable. But with the number of entities on NIS you cannot know them all* (respondent 7). Moreover, this respondent focused on the traffic light protocol, meaning that how far you are allowed to use the information is relevant in the process. In this line, another respondent said that you cannot share everything with everyone, otherwise the trust is hampered (respondent 5). Therefore, informal processes such as trust and compliance are juxtaposed with formal processes such as legislation.

Also, respondent 7 said that the *sectoral approach and the need to combine more cybersecurity knowledge with people that know and/or are close to the sector* is relevant to take into account. Therefore, a main finding in this regard is that information sharing is key when is voluntary and when the spread of knowledge is allowed because there is always something to learn from other activities made by other entities alike.

According to other respondent, the reporting on the threshold is relevant when analysisng information sharing by entities, the respondent said that *non-government parties receive information from entities* more from the government, but also other entities *and report obligations as of October 2024, whether they are reaching the ideally* (respondent 3). Also, this respondent argued that *the government has gained the trust and that* according to *the Wbni* there are *a few articles that prohibit the notion of secured data for a specific service provider.* According to this respondent, the information is private to a certain extent (respondent 3). Conversely, this respondent also stipulated that the information is disclosed, therefore it seems rather blurred the lines of whether the Dutch governmental institutions disclose or not the information and how much the government actually discloses. According to the Wbni (2018), both vital and digital service providers are required to report incidents that have significant consequences for service provision not only within the Netherlands but also in other Member States. Additionally, as stated in Article 3(d) of the Wbni, the government, during the data processing of the reports, may share this information with other government bodies (sectoral ministries, CSIRTs, and so on). This sharing of information serves the purpose of informing and advising service providers, both within and outside the Netherlands, about potential threats and incidents.

Respondent 3 *said that when* dealing *with a private company or organisaiton, we are talking about pushing information,* therefore for their organisation a trustworthy network is important since their network is broad, and when sharing the information the trust in the information they are providing as well as non-disclosure of whom has provided the information is key (respondent 3).

Furthermore, another respondent stipulated that *information sharing is not something that we do* (respondent 2). Therefore, the information in this case is rather private. Furthermore, the respondent highlighted the disparity in information-sharing practices among various organisations, entities, or companies in the Netherlands. It was revealed that some organisations are indifferent to the risk of their data being stolen (because their information is publisised), while others emphasise the importance of data security due to the pivotal role it plays in safeguarding their financial operations and maintaining the confidentiality of their processes. Therefore, according to respondent 2, is a case-to-case basis whether information-sharing schemes are in place and consequently, transparency.

Moreover, according to respondent 4, the focus is more on the collective effort at national level. *There are a lot of meetings to benchmark our efforts and share information* on how regulatory bodies need to act. Respondent 4 also said that currently, they find themselves in a transitional phase as they move towards the implementation of the NIS2 Directive and its integration into national law. Also, the Ministry of Justice is the main coordinator bringing together all the relevant ministries involved in NIS2. This respondent explained that formalised meetings are taking place to facilitate information-sharing schemes, indicating that practical steps are being taken to ensure coordination among the competent authorities in the Netherlands. Therefore, the key point is that the aim is to harmonise the approaches of these authorities for the implementation of the NIS2 Directive in the Netherlands.

According to another respondent, the private sector in Member States, *must do what they can to promote vulnerability management in the organisation, and vulnerability disclosure* (respondent 6). Therefore, it is implied that the legislation made at the EU level can be helpful for the private sector in the Netherlands regarding the disclosure of information. In the Directive, CVD policies and European databases are aimed for. However, this is still in its infancy.

Lastly, according to another respondent, within their *organisation we have those lines where we communicate proactively. We are trying to be as open and transparent as possible* (respondent 8). Moreover, this respondent said that they *use NIST and* other standards *to share the information for the technical stuff.* If any incidents occur, communication takes place via email or phone calls and the cooperation and collaboration with these organisations occur on a monthly basis (respondent 8).
This respondent explained that as a way to share information and also knowledge nationally, within their company they try to assist other organisations in the interpretation of the Directive's mandates*, the bigger organisations helping the smaller ones,* dealing *with cyber and* sharing *knowledge and risk-management approaches* (respondent 8). Therefore, this respondent stipulates that information-sharing schemes are relevant and spillover of knowledge across the industry is crucial in the Netherlands.

Finally, according to the report CSAN (2022, p.17) in the Netherlands there is fragmented incident response, insufficient supervision, and inadequate sharing of information. Overall, information sharing nationally is centralised in NCSC, but when it comes to share information among organisations the process gets more complicated. The reasoning is twofold. Firstly, the need for a trustworthy network is key. Secondly, transparency of the information might differ when dealing with a public or a private entity and also when being directly related to the Dutch government. Consequently, information sharing is something that seems to happen within entities that are similar to each other (horizontal level), but not in a vertical level. This raises a lot of questions. However, it is expected according to the *'Literature review'* section that different governance models coexist and that the cybersecurity sphere is highly contested because a big amalgam of actors is involved. Therefore, the main finding is that it seems there are information-sharing schemes within the network of governmental institutions on the one hand, and within the network of companies or entities, on the other. However, when it comes to information sharing between government - entities, the trust levels are lower or the information sharing only happens regarding a specific threshold agreed upon by law. Moreover, information sharing and trustworthy networks go hand in hand, for which almost all respondents agree. The existence of trust within the system enables the sharing of information within that system. However, when it comes to Dutch governmental institutions, the levels of transparency become unclear and ambiguous.

b. Information sharing (EU level)

Information sharing at the EU level is understood as the process of providing the network with information regarding incidents or risks, as well as information on ISMS or best practices among EU institutions, but also from these institutions towards the public authorities in Member States or the private sector, specifically in the context of the Netherlands. Therefore Coordinated Vulnerability Disclosure (CVD) policies have been a recurrent topic in the interviews. The main finding has been that information sharing is a result that organisations at the EU level with the national authorities in the Netherlands want to achieve, but often transparency issues arise, making the information not easily accessible. Moreover, some respondents argued that ENISA should be the main reporting body at the EU level, for which one report will be done instead of multiple. It has also been observed that at the EU level, the trialogue process during the negotiations is quite

relevant in the case of Directives like the NIS2 Directive under review in this study. This is the case because in the trialogue process, information is shared and multiple meetings with different bodies happen. Therefore how that information is shared and with whom not only may impact the process but also may hamper the possibility of a trustworthy network.

Now, some specific examples of the respondents' answers will be provided to give light on this specific topic. Trust and information sharing at the EU level are relevant as well as at the national level. One respondent said that *trust is also something that we try to increase and promote in meetings and workshops. This is also why we try to bring together the public and private entities. This takes a big role in information sharing, in instant reporting, and in proactiveness* (respondent 6). This respondent emphasised that in their organisation's activities, trust was something they were aiming for. Another respondent said that *it is very important the trust between the* organisations because if they think that we have been having contact with other organisations behind their back, without them knowing, *could backfire on us* (respondent 5). Consequently, there is a need for precaution regarding what and with whom you share the information at the EU level, because that might impact the trust processes within your network.

Secondly, respondent 6 argued that some organisations do not have CVD policies, tus considering a scenario where, as a researcher, you discover a vulnerability in a product but find no contact information on the website. After sending an email with no response, you decide to publicly disclose the vulnerability. However, this action can have significant negative consequences, such as malicious actors exploiting public information right away. Therefore, this respondent emphasised that the national policy aims to establish a secure and responsible framework for disclosing these vulnerabilities (respondent 6). In a way, it can be argued, that information sharing and making data public is a double-edged sword. It seems that information sharing needs to go hand in hand with trust, simultaneously trust in topics such as cybersecurity is highly contested because multiple actors are involved and in the case of the NIS2 Directive. The scope broadening is imminent, not only at the national level, but also at the EU level. Consequently, trust might be hampered.

At the EU level, another respondent named the Cooperation Group in light of the NIS Directive, the respondent said that *the Member States exchange information on the implementation of the notification obligations, but also on the security requirements* (respondent 7). Moreover, when talking about the need of a trustworthy relationship within the network, this respondent said that *finding a balance might be a challenge*, regarding the increase of organisations due to the NIS2 Directive. Also, *it is still to be analysed to what extent the broadened scope is going* to impact the information sharing *in practice or to what extent ENISA is going to be able to make CVD guidelines* (respondent 7). Therefore, information-sharing schemes at the EU level is still to be analysed.

Regarding the role of ENISA, another respondent said that more guidance from ENISA was needed, meaning *that every MS is working on formats and guidelines, but it will be more efficient and effective if there was one sole report and therefore ENISA could be helpful, but it needs the resources* (respondent 4). Consequently, information sharing at the EU level could be centralised in ENISA, to make the processes more effective according to this respondent.

Another respondent said that the information sharing at the EU level happens with the bodies of interest for the specific industry, *each of those bodies has a periodic meeting, and the EU body for our sector* is the most important meeting for them. *Within that body, we work together on the new legislation,* and *the Directive* (respondent 8). Consequently, the information sharing at the EU level works horizontally, with organisations that are alike (both in nature and regarding the sector) according to what has been said by this respondent.

Overall, information sharing at the EU level is scattered among EU bodies for each sector, the NIS Cooperation Group, ISACs, and ENISA to a lesser extent. This is important for the Dutch case because the Netherlands is represented in and an integral component of these networks. At the EU level, a trustworthy network is also significant, but difficult to achieve due to transparency and trust issues, so the process gets complicated. Consequently, information sharing is something that seems to happen within entities that are similar to each other (horizontal level), but not in a vertical level. This is also seen at the national level with governmental entities and the private sector. This raises a lot of

questions and implies that more joint effort is needed to establish ENISA as a main reporting place as well as the development of CVD policies and guidelines for Member States, which could potentially benefit the Netherlands as well. It seems that the information-sharing processes at the EU level are rather decentralised, therefore entities do not know exactly to whom to address certain issues. Consequently, the national level and sectoral entities take over the information-sharing processes.

c. Coordination nationally

Coordination nationally is broadly understood in this study as how governmental institutions and the public and private sector coordinate their approaches regarding cybersecurity risk-management measures to achieve a high common level of cybersecurity in the Netherlands. In this regard, it is important to note that in the interviews conducted, the term coordination and harmonisation have been used as synonyms. This might create an overlap with one factor of the *'Enforcement effectiveness'* section, which is *'Uniformity'*. However, in this study, the consideration of the uniformity factor comes as a result of whether or not there is coordination and harmonisation within the governmental institutions' approaches to cybersecurity risk-management measures, and, to a lesser extent public and private sector approaches.

The main findings have been that the main coordinator for the implementation of the Directive in the Netherlands is the NCTV within the auspices of the Ministry of Justice and Security. Moreover, it has been inferred from the interviews that even though the Dutch government acts as one, the different sectoral ministries act in practice differently and that sometimes coordination seems difficult to reach. In this regard, one respondent said that in the Netherlands there is no grand scheme, that there is a clear divide between CSIRTs and competent authorities, but that that might be different in other countries. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic.

Firstly, according to one respondent *we try to harmonise approaches but of course in every organisation that is always a challenge, for the entities they seem one central government, acting as a whole, but it is different parts of the body* (respondent 1). Moreover, there is *a combined effort of all* Dutch governmental institutions *within the*

Netherlands to come to a general view of the current level of cybersecurity. According to this respondent, *there is a group with all the different cybersecurity supervisory authorities in the Netherlands,* thus they come together to achieve consistency, ensuring that their activities are not in conflict with one another (respondent 1). Therefore, coordination happens by trying to reach common ground in the measures in place in the entities.

The topic of harmonisation is under *discussion from the ministries, e.g., what do we harmonise and what do we make sector-specific, and then how do we organise that legally* (respondent 1). In this regard*, with the implementation of lower-level laws. We will contact the other bodies to write down more specific lower-level legislation* (respondent 1). This respondent emphasised that within the government there are different parts to the same body and that is a challenge. Also, a relevant point made is that *even with the same law, the same measures, and activities, how you actually* use/choose measures *might differ between organisations and the way we act on them* (respondent 1). Consequently, a main inference is that cooperation is aimed for, but in practice, the way the structure works makes the aim difficult to achieve.

Secondly, according to another respondent, *every group within their organisation has its own specialties, there is some overlap but not in* all the parts of the organisation (respondent 2). Regarding this, the interviewee emphasised that cooperation with other organisations exists, but it is up to each part of the organisation and it works at a different pace. In this case, specifics about cooperation nationally with governmental institutions were not further discussed.

Thirdly, another point made is regarding the coordination nationally being done by NCTV's role. Respondent 3 said that their *organisation has tight working relation with other departments, e.g., Department of Economic Affairs, but also Department for General Affairs and for Defense. We have to coordinate with the target groups that are vital organisations and Dutch central government, and the vital organisation are in the care of the Ministry of Internal Affairs and the Dutch central government.* This respondent emphasised that harmonisation is key in the NIS2 Directive when comparing it with the NIS Directive. Therefore, the coordination is made by NCTV, but it is in its

infancy regarding NIS2 Directive and it will be further analysed once the Directive is transposed into national law.

Another respondent also focused on the fact that harmonisation in the Netherlands is key. This respondent said *that there are a lot of meetings to benchmark our efforts as regulatory bodies. The different departments are meeting regularly to develop interdepartmental collaboration for policy and inspectorates* (respondent 4). Therefore, the meetings mentioned allow for harmonisation in the measures implemented by the different sectoral ministries, which implies that the first steps towards uniformity are being made (which will be further explained in the *'Enforcement effectiveness - factors'* section). However, the fact that the NIS2 Directive is yet not transposed into national law has been exposed as a deterrent and the effects this might have on the Netherlands will be further analysed in the near future. However, whether this is how it will go, it is still to be seen.

According to respondent 5, *we had a really clear team, we were working closely together* and it worked well together. This respondent also emphasised the good connection and group environment within the DORA and the CER teams. This respondent stipulated that there is a team effort and full confidence in the process. Their organisation has talked to everyone. This respondent referred to the Permanent Representations when talking about national cooperation and the interview subject said that *there is a minimum level of harmonisation* (respondent 5). However, when being asked about possible challenges such as misunderstandings or not reaching a common ground within the team, the interview subject that that was not the case. As the main finding seems that coordination and conversations are flowing, but that does not mean that actual coordination at both the national and EU levels happens in practice, thus much more analysis is needed.

In addition, another respondent emphasised that they *are trying to harmonise and make it easier for the 'good guys' to do their work* (respondent 6). In this regard, *to help this harmonisation by putting out guidelines and good practices* for the Netherlands and other Member States to promote harmonisation in the implementation of the Directive. Moreover, according to this respondent a learning outcome and a way of harmonising within NIS2 *is to achieve a greater harmonisation in how the critical entities are identified in the Member States, to establish better the baseline security requirement for*

these entities. Therefore, harmonisation is aimed at, plus coordination with sectoral parties within the Member States.

Lastly, two respondents emphasised the room for interpretation of the NIS2 Directive (respondents 7 and 8). The main idea is that the mandates are quite prescriptive with NIS2 and *that will also make a difference to the harmonised manner of* implementation (respondent 7). As a counterargument to this, another respondent said that *you want harmonisation but you also want some flexibility* (respondent 8). More concretely, respondent 7 focused also on the relevance of the NCTV. *This is done in collaboration with all the sectoral ministries.* The interviewee said that they *created a team with two colleagues that sort of coordinated the whole negotiations. So we have also been publishing ideas before the NIS2 Directive was published and during the whole process we have also coordinated inter-ministerial* work *between the agencies making sure our input was well represented.* This respondent emphasised that with the new national cybersecurity strategy, the idea in the Netherlands is to go to a more centralised approach because now it is rather decentralised. In this regard, there are a *couple of sectoral computer security incident response teams* in the government, *the health sector has one or the water management sector, and they also collaborate with the NCSC and an informal network* (respondent 7). Therefore, it seems that coordination happens more horizontally, meaning within the sectors rather than vertically, meaning other sectors and private entities from those sectors.

Lastly, another respondent specified that there are national and international networks of cooperation within their organisation. In this regard, respondent 8 stipulated that national network of cooperation is always happening because their organisation is under the magnifying glass, therefore all knowledge and assistance becomes imperative. In this line, their organisation cooperates with EU bodies for their sector and *within that body, we try to help the other organisations to interpret* the legislation: NIS2 and others (respondent 8). It is important to mention that according to this respondent, this happens both nationally and internationally.

All in all, coordination nationally is something that is happening in the Netherlands. However, different measures are in place and different bodies are part of the government, this complicates the full coordination and harmonisation of the measures/approach taken

by the Dutch government. Nevertheless, it seems that when it comes to the sectoral ministries, the communication between these ministries and the industry is ongoing and relevant in the negotiations. Consequently, coordination is something that is happening in the Netherlands, and generally speaking, people know who the main coordinator is and what to expect from different entities and bodies. However, in several meetings attended in which medium-sized and small-sized companies were invited, the general approach was completely the opposite. Therefore, it really depends on whom you are talking to, the sector they are part of, and the resources they have at their command, to see the approach they take towards coordination, collaboration, and harmonisation in the Netherlands regarding cybersecurity risk-management framework and its measures.

d. Cross-border cooperation

Cross-border cooperation in this study refers to both cooperation within the EU and also internationally. In general terms, this cross-border cooperation has been referred to as the NIS Cooperation Group. Moreover, the role of the Permanent Representations of the Member States plays an important role in cross-border cooperation as well. In general, the EU sectoral networks have been also mentioned. Therefore, cross-border cooperation seems to be happening at least regarding meetings within the different networks. This factor has been further explained in Chapter 2. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic.

First of all, respondent 6 said that their organisation *tries to foster harmonisation in this implementation among the Member States*. This respondent said that the NIS Cooperation Group is key in this process, it *is a strategic instrument* in which Member States *work together to coordinate their efforts in the implementation of the Directive*. Within this group, *there are work streams, sectoral work streams, horizontal work streams that are working on aspects of NIS2 that are applicable horizontally, security measures, and vulnerability disclosure. These are applicable to all areas of the economy,* coming up with guidelines and policies, and so on. This work aims *to be more harmonising* with what the Member States implement, for which they *get together and exchange experience and expertise* (respondent 6). Therefore, cross-border cooperation is aimed for, not only at the operational level, but also at the organisational level, to raise awareness, and share knowledge. Also, within cross-border cooperation, the precondition of harmonisation discussed in Chapter 2 is key.

In addition, according to respondent 7, *in the Cooperation Group the Member States exchange information, on the implementation of the notification obligations, and also on the security requirements, to ensure more harmonised implementation. For NIS2, the Netherlands* follows a *precept approach and we are going to work together as the European Member States and the Commission to this implementing act for more digital infrastructures.* This respondent also focused on the *CSIRTs network for which NCSC is the representative in the case of the Netherlands* and the respondent also stipulated a different *network: EUCyCLONe, a big cyber-crisis management network on the technical strategical aspects*. This respondent emphasised that the *Cooperation Group is the main outlet where it is being discussed how the NIS2 can be effectively implemented in a harmonised manner*. In this regard, the idea was also regarding the fact that it is beneficial for Directives when the experts that are drafting the laws in each Member State are exchanging views at this stage towards the implementation, rather than still being discussed in the EU institutions. Other respondents also emphasised the idea that in Brussels other files are being considered at the moment (respondents 5 and 7), rather than the NIS2.

Moreover, respondents 1, 2, and 4 focused more on national cooperation rather than cross-border, some examples were made but that do not add more information to what has been already explained. According to respondent 3, within their organisation, *we have a quite good work process for cross-border cooperation with the Union that already existed* with the NIS Directive. This respondent said that certain challenges *arose in the cross-border cooperation which is outside of the EU, with outside servers executing processes, e.g., in Asia, America, or Africa*. The respondent also emphasised the problem that arises, which is *problems of interpretation of the law as the competent authority, state IP addresses, there are different levels of digitalisation,* also in the EU *there are different levels of digitalisation, e.g., Romania* (respondent 3). This respondent highlighted that in the context of telecommunication networks, the absence of borders adds complexity, particularly when there are disparities in digitalisation levels and legal understanding. Consequently, it can be deduced that greater international cross-border cooperation is necessary, and although the EU is making efforts in this regard, certain Member States still lack adequate resources for cybersecurity measures. This becomes problematic when online services operate without regard for borders.

Other interviewees stressed the cross-border cooperation happening in the Council and the NIS Cooperation Group in which a lot of different Dutch governmental institutions participate (sectoral ministries). In this regard, respondent 5 said that *negotiating between Member States is happening in the Council*, in here *the Ministry of Justice and Ministry of Economy, have given their views on the* NIS2 Directive's mandate.

Lastly, regarding the views on cross-border cooperation, respondent 8 said that *the advantage of being within the industry is that there was a need to collaborate internationally. So we have all kinds of bodies globally and European bodies that are working on safety and rules of the specific industry we are part of.* This respondent also said that *within the body* of our interest: the EU bodies for our specific sector, *we work together* (respondent 8). Consequently, it can be inferred, that cross-border cooperation is something that according to this respondent is happening and that all the resources and energies are put into it within the network of entities that are alike, notwithstanding their size.

Overall, cross-border cooperation is seeing in work streams such as NIS Cooperation Group, the CSIRTs network and other networks in which alike organisations come together to reach common grounds regarding cybersecurity risk-management approaches, share knowledge and practices, as well as guidelines and policies of different nature with the end goal in mind of achieving a high common level of cybersecurity in the EU. In this regard, one main finding is that depending on the organisation, cross-border cooperation is seeing differently. The nature of the organisation, the resources, being public or private differs on the approach taken towards cross-border cooperation as well as in the answer given by the respondents. All in all, the Netherlands seems a country quite preoccupied with the topic of cybersecurity, therefore all resources and energies are put on it.
Therefore, in certain cases cross-border cooperation happens just by talking with everyone, while for other individuals and organisations, cross-border cooperation arises from the collaborative efforts of sector-specific work streams, working together to align their approaches in addressing risks and incidents on a regular basis. This cooperation serves as an initial stride towards the successful implementation of the NIS2 Directive in the Netherlands. In this regard, cross-border cooperation allows for Member States to

share knowledge and practices with each other, which allows for a first step towards the 'effective' implementation of the NIS2 Directive in the Netherlands.

e. Public-private cooperation

Public-private partnerships are aimed at in the Netherlands, but in practice, this is still an ongoing process that is in need of more development. For those entities that have their services internationally, both cooperation and information sharing are difficult to fulfill because of two reasons: i) different levels of digitalisation, ii) different ways of understanding the law.

First of all, respondents 1 and 2 talked about cooperation and collaboration in a broader way rather than specifically regarding public and private cooperation. Secondly, according to respondent 3 within their organisation they *are working on project-based cooperation but there are always things to overcome because as the government there are certain obligations such as disclosure.* Therefore, it can be inferred that cooperation is happening but it is not finalised yet. Moreover, the interview subject said that *when we cooperate with a private company, this private company has the freedom to get some service company to help* with different services that they might need (respondent 3).

Thirdly, respondent 4 when being asked about the coordination of his organisation with the private sector said that *there were four-times-a-year meetings to the awareness and resilience at a different level, and guidelines to help them on conducting their own investigation* (respondent 4). Therefore, through different meetings, this cooperation between the public and the private sector was achieved.

In addition, according to respondent 6, within their organisation they try to foster this cooperation. However, they said that at the moment they are only working with the public authorities. The interviewee said, however, *that there is a lot to be gained* from *the public-private sector cooperation because there is a lot of expertise to be shared from both parties. There are a lot of sectoral ISACs, so we try to create communities where there are public and private members both present so they can engage with each other.* Another interviewee also said that NCSC has a lot of collaboration networks with the industry, *with ISACs. They have them for 14 sectors,* reason why *they collaborate with different entities, private organisations* (respondent 7).

It was interesting to see that another respondent said that *the private sector sees cybersecurity as a way for market differentiation, and potential advantage in their products and services*. *While the public sector is trying to protect the market, the citizens, the public, and the economy* (respondent 6). Therefore, the point taken was that even though the main goal is to create that cooperation, *there might be some kind of disengagement.* This may hamper the effective implementation of the NIS2 Directive in the Netherlands, since certain European and international standards are developed by the private sector, and both sectors should be aligned in their measures and approaches since cybersecurity risk-management impact both sectors in the Netherlands. Moreover, the interviewee said that they *organise forums or conferences where* they *invite private speakers* and *public authorities.* Giving *them a chance to listen to each other, to engage, to collaborate* (respondent 6). Therefore, the differences between public and private entities are imminent, but the collaboration of both is needed, because the public authorities have the enforcement capacity in the Netherlands while the private entities have the resources and knowledge at their disposal, which can be beneficial for the implementation of cybersecurity risk-management measures in the Dutch critical infrastructure.

Another respondent said that *on a national level, there are different structures in place. So you have like something called the Commission for Critical Infrastructure, which is chaired by NCTV and the sectoral organisation for companies*. Moreover, this interviewee added that they are working on a broader network of meetings to involve companies. In this regard, all the sectoral ministries talk a lot with the sectors in ad hoc or structural format (respondent 7). Moreover, the respondent made the point that if you as a company work in different countries, *if you know the CSIRTs have a certain level of cybersecurity and adhere to the same standards,* that might be helpful. *So they have a harmonised approach that when you trust the system, you also trust the people working in it.* Therefore, from the standpoint of a company, greater harmonisation is preferable since it allows for the adoption of consistent measures within the network. Furthermore, a reliable network plays a crucial role in facilitating this cooperation.

Lastly, according to respondent 8, within their organisation *they use NIST* and other standards to facilitate the sharing of technical information within the organisation. Also,

we just email the other organisations in the public or private sector *or call them if anything happens.* Moreover, this respondent added that cooperation and collaboration with these organisations happen *on a monthly basis. I think we have a close cooperation with our other partners here* in the Netherlands*, at the European and national levels.* Therefore, it seems that private-public cooperation happens and constant contacts with partners and other organisations within the network of the sectors are crucial.

All in all, public-private cooperation seems something that is aimed at in the Netherlands. However, the extent to which this happens is still under debate. Actually, it seems to happen more at the EU level with networks such as the CSIRTs or NIS Cooperation Group or sectoral work streams rather than within the national system per se. Of course, we cannot forget that trustworthy networks and good relationships play a major role in public-private cooperation. In addition, some respondents added that these partnerships are relevant and needed to work on because the public sector could be highly benefited from the knowledge and resources of the private sector in the Netherlands. As a result, this could lead to the effective implementation of harmonised cybersecurity risk-management measures at the national level due to the promotion of coordination and cooperation between the public and private sectors.

5.3.2. Enforcement effectiveness - factors

This section will provide a detailed explanation of the primary findings pertaining to each factor included in the *enforcement effectiveness* theoretical framework of this study, as outlined in Table 1 above. Additionally, the preconditions necessary for establishing these factors initially, as presented in Table 2 above, will be elaborated upon.

a. Personal and institutional liability

In this section, personal and institutional liability is further explored. It is important to mention that under the scope of NIS Directive personal liability is not considered and in this case, some respondents were unwilling to share their views due to not knowing the effects just yet (because NIS2 Directive is still not transposed into national law). However, some insights and considerations were provided. Generally speaking, the respondents agreed on the effectiveness of the measure, but consider that depending on

the size and resources of the company these fines will have the desired effect or not. Therefore, some respondents considered that the fines should be a last resort thing and should be implemented for those companies that after a period given are not doing good and have not improved. Therefore, some respondents considered that other methods needed to be in place before fines and that not only the fines would make the change. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic.

The moment there is the possibility of fines, *the method* could potentially *make the entities less willing or less open to sharing the information. So it may have a reverse effect.* In this regard, this respondent said that only giving fines is *maybe not the way you want to improve digital resilience so that might not be a path that you want to take* (respondent 1). According to this respondent, it is crucial for the measures implemented to be tailor-made. Therefore, various approaches can be employed, such as issuing binding instructions that specify required actions (which may involve a burden under administrative coercion and penalties). Prior to resorting to such measures, soft controls can be exercised by avoiding actual fines and instead providing reports to the responsible parties, granting them an opportunity to react to the fine. If the necessary measures are taken within a six-month timeframe, no fine would follow. However, if no significant improvements are observed after this period, more stringent measures may be implemented for the parties involved. Consequently, according to this respondent, different procedures can be fulfilled before an organisation is actually fined. But this should be a last resort procedure commanded by the national government authorities. In this line, respondent 4 leveraged the fines being a last resort measure and that it comes when organisations do not report the incidents.

Secondly, according to another respondent, *fines can be effective, but I also agree with the hesitation of 'this is not going to happen', because people will lawyer up and they will make sure that they will not be held liable themselves* (respondent 2). In this line, respondent 3 said that with the NIS2 Directive not only the *cybersecurity departments of an organisation,* but also *higher positions* within that organisation are *interested in this Directive due to liability* purposes (respondent 3). However, respondent 2 argued that the liability can be an incentive since it is *up to law enforcement to endorse it*. However, if the thresholds are low organisations might do a cost-benefit analysis and opt to simply

pay a monetary sum to ensure compliance with cybersecurity measures. Their decision-making would be based on comparing the cost of implementing cybersecurity measures against the potential fines, ultimately choosing the option that results in a lower financial burden. In terms of personal liability, this respondent said: *I hope there will be a better incentive for both management and actually doing something with cybersecurity* (respondent 2). Consequently, according to this respondent, the usage of fines is double-edged. It can also be argued that the resources and levels of maturity of the organisation in question may influence the approach taken towards liability.

When talking to respondents 5, 6, and 7 the personal and institutional liability and the measure of fines imposed by the NIS2 Directive did not pop up. However, other measures were considered and they were aware of liability under the NIS2 Directive. In this regard, respondent 5 also referred to a draft of the NIS2 Directive directed to EU institutions, because under this Directive these institutions are not liable. In this document it is said that 'Member States called for further alignments with NIS2, more reciprocity in the exchange of information between the Union entities and the Member States and pointed to the excessively voluntary nature of some of the proposed measures' (COD 2022/0085, paragraph 9). Consequently, it remains to be seen whether this Directive will also yield implications for the EU institutions.

Lastly, according to respondent 8, when being asked about 'fear' of reporting due to the possibility of getting fined, the respondent said that in their organisation, *they are not afraid*. *We have a good understanding with NCSC.* The respondent further mentioned that they maintain a good understanding with the regulator. When it comes to reporting to the regulator, they strictly adhere to the mandatory threshold as required by law. However, if there are significant concerns or incidents, they take a proactive approach and report to the NCSC, sector-specific entities, or other European counterparts that share similar responsibilities. Given the nature of their organisation, they prioritise openness and transparency, aiming to uphold their sense of responsibility (respondent 8). Therefore, it seems that the actual reporting happens to the NCSC or the sectoral entities alike, rather than to the competent authorities per se. The latter only happens when it is required by law. It could be inferred that the trust is based on the NCSC as the gatekeeper of the information for the entities.

Overall, fines seem to be a good incentive for organisations to implement cybersecurity measures. However, it is a double-edged measure since the possibility of fines can be beneficial or an incentive while making organisations less transparent and less willing to share the information as well as doing a cost-benefit analysis regarding whether paying the fines or being secure as an either-or position, to assess what is a more suitable option for them. Another finding has been that fines are the last resort measures, usually, there are other measures in place, so then organisations have various options to revert the situation before getting fined. Consequently, liability allows for all areas of the organisation to be aware and take into consideration the Directive's mandates regarding cybersecurity risk-management. Therefore, this is a factor that allows for a step further in the effective implementation of cybersecurity risk-management measures in the Netherlands. However, this factor solely does not ensure effective implementation, but other factors and preconditions need to be considered.

Lastly, another finding is that the fines come more when organisations do not report their incidents, for which trust plays a key role, so it has been a general idea that the reporting of incidents is to NCSC because there are no consequences (in the form of sanctions for instance) and the reporting to the regulators happen when it comes to the threshold stipulated by law. Therefore, when it comes to liability certain preconditions already analysed in Chapter 2 come to play their role.

b. Repellent enough to cyber-risks

After conducting the interviews, it has been a general approach that the Netherlands is repellent enough to cyber-risks by being certified by either ISO 27k series or NIST. Some respondents argued that more than being certified is needed to be actually secure and others also stipulated that there is no 100% security and there is always something to improve. In general, it appears that organisations in the Netherlands are repellent to cyber-risks. This is the case because according to the respondents last year no important risks were reported. However, there is an ongoing debate in which the risk-based approach is being juxtaposed to compliance, thus whether being compliant with NIST or ISO is enough in cybersecurity. If we take into consideration the CSAN report, basic measures are insufficiently implemented in the Netherlands. This concerns the use of multi-factor authentication and creating tests and backups (CSAN, 2022, p. 18). Getting vulnerabilities under control and keeping them under control is part of risk-management

(CSAN, 2022, p. 22). It is important to note, that this factor is highly interrelated with the preconditions analysed in Chapter 2: risk-based approach and compliance. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic.

In this line, the measures taken by the respondent's organisations are as follows according to respondent 1 *we take into account the risks that we see or we get from external partners.* In this regard, this serves as a basis to implement measures to try to avoid that effect in the future. Moreover, according to this respondent, it is about a culture within the entities, therefore *they know they have the responsibility to take the measures, to manage their risks, and also that you are never done with your cybersecurity*. In this regard, within their organisation they *want to create posture with the entities, they should internalise the importance of cybersecurity.* Doing this *by first looking at best practices like ISO standards.* But how this will be for NIS2 Directive is still under debate, what they see within their organisation is that *most of the organisations have ISMSs*, and *they have a governance structure to implement it. From there they take measures to mitigate the risks.* The respondent finalised saying that they *think awareness and the willingness to mitigate risks and to look at them from the company perspective is more important than only compliance with the law.*[9] Moreover, this respondent specified that *they do see the use of best practices, e.g., ISO27005* as leading an example of risk-management. Consequently, by having their measures up-to-date and raising awareness within entities cybersecurity is a priority for all, rather than only for the cybersecurity departments within the organisations. Therefore, the implementation of the Directive is a combined effort of all sectors and organisations of different kinds.

According to respondent 2, a lot of measures implemented in their organisation are done by skilled technical employees, but the human factor is also something that they take into consideration. Moreover, the respondent provided with specific examples of reducing risks within their employees, e.g., *not granting administrator access to their company laptops to reduce the risks involved in such access.* Therefore, it seems that the responsibility is placed on the employees rather than on the organisation's system or

[9] This was, however, a personal statement.

policies in place. However, the ISMS was not disclosed for reasons of confidentiality, thus no more analysis can be provided in this regard.

In addition, another respondent said that the aim is to *implement the measures mentioned in the second paragraph of the NIS2 Directive. But there is cyber-hygiene* and *they are still discussing that* because this is a confusing concept. This respondent also stipulated that according to the *number of incidents and the consequences, entities need to be assessed.* Also, *sharing general practices and ideas, can help entities and organisations* to be repellent enough towards cyber-risks (respondent 3). Consequently, information sharing and policies that help organisations seem something relevant towards being repellent enough towards cyber-risks. Sharing information not only enables the dissemination of knowledge about specific risks but also has the potential to mitigate or prevent those risks from occurring.

Furthermore, according to respondent 4, their role is important to ensure that *more organisations in our domain have their safety in order. We provide an overview of what we see in the cyber-image of the joint supervisors,* which will focus *on drinking water supply, flights, and aircraft handling*. Moreover, this respondent specified that within his organisation *investments have been made and a new cybersecurity department has been launched to further expand the* cyber *capacity*. Therefore, efforts within his organisation are being made to be ready organisation-wise. Moreover, this respondent focused on standards such as NIST and ISO and the need for tailor-made approaches for each sector. However, he also specified that standards cannot take over the supervisory activities, because being compliant does not mean being secure (respondent 4).

Moreover, respondent 5 focused on the reporting timelines and its consequences. This respondent emphasised that *it is not just going from incident to incident, but what* my organisation *really wanted to establish, is a certain awareness of the issues regarding cybersecurity in general.* Therefore, *an organisation would include training for all of the people working in all cybersecurity-related matters* (respondent 5). *The Dutch government when it implements the Directive, will explain* the specific definitions. Moreover, this respondent focused on: *the idea is establishing a general awareness of cybersecurity, so the NIS2 brings more rules, but the rules are needed to solve issues faster* (respondent 5). This respondent emphasised the importance of ensuring that all

parts of the organisation comprehend cybersecurity and that the responsibility lies with the national authorities to establish the minimum definitions and common concepts in light of the Directive's mandates. Moreover, that the reporting periods might impact how the information is shared and whether the incident is properly tackled.

According to respondent 6, their organisation's publications *do help policymakers and the industry see what are the threats that we are dealing with and how to prepare for them*. This respondent specified that within their organisation they *have different publications (studies or reports) and they have done a recent analysis of various risk-assessment methodologies, we provide good practices in several areas, also we provide sectoral advice for telecoms, for core Internet, and/or for the cloud.*
Moreover, this respondent said that they *provide cybersecurity expertise to help them develop cybersecurity policies in the right way,* by providing *cybersecurity expertise, but* also by supporting *Member States with the implementation of this policy*. And along with that, they try to foster harmonisation in this implementation (respondent 6). Lastly, this respondent emphasised that they *are certified in and try to be compliant with ISO and NIST standards as an organisation internally and also they deal with cybersecurity incidents and basically work with the Member States and the NIS network in dealing with these incidents*. Likewise, within their organisation capacity building is relevant, so among their purposes, *they raise awareness, improve education in cybersecurity matters and provide good practices in many areas around cybersecurity.* Consequently, once again raising awareness and sharing policies and knowledge seem to be the way this organisation tries to work within its network to repel cyber-risks. Therefore, preconditions such as risk-based approach and compliance come to the front when dealing with the factor of repelling cyber-risks in the Netherlands.

According to respondent 7, being repellent to risks depends to a certain extent on the risk-based approach, *so which are the risks faced? What kind of data do they have? This risk-management measures since the whole system is designed* as follows*: you have your supervisory authorities and enforcement measures. They are the ones that can check whether or not you have done everything you can to prevent an incident in a case-by-case analysis*. Consequently, the risk analysis is key to understand the type of risks your organisation needs to work towards as well as being alligned with your CSIRTs standard-wise, so the measures are harmonised and the vulnerabilities are taken into account.

Consequently, harmonisation and risk-based approach come to the front according to this respondent. This respondent also mentioned standards such as ISO 27001 or NIST.

Lastly, according to respondent 8, the fact that each day everything is becoming more automated, has consequences for their organisation, *because it comes with a cybersecurity risk, which we recognised as a top ten risk within our organisation. And then we say, if we want to be successful digitally, we need to spend enough attention, time, and resources on cybersecurity as well.* This respondent said before they were less mature and with time their maturity levels got higher, also that *one person got responsible for cybersecurity and then we started to put more and more effort into cybersecurity as the digital program grew*. This respondent explained that they wanted to go along *with other critical infrastructure and with financial services* and for that reason, they were aiming for specific levels of maturity (respondent 8). Therefore, it can be inferred that being repellent to cyber-risks is aimed at.

This respondent also explained the process to become repellent toward cyber-risks, by rating the risks and getting their risk profile. After this occurs, they assess the appropriate actions to be taken and establish various levels (such as low, acceptable, and high risk) within their policy. The respondent emphasised their desire to enhance their cybersecurity capabilities, aiming to be internally motivated rather than solely reliant on NIST or ISO standards. However, they acknowledge the necessity of conforming to these standards. With the NIS Directive, they can adopt a risk-based approach that aligns with their own expertise and professional judgments. Therefore, standards and general practices widely accepted within their sectors are taken into account as well as a risk-based approach in which the risk analysis, risk profile, and risk appetite are taken into consideration.

Moreover, *in the workplace they need to automate everything, but it is so hard to get everything up-to-date all the time, therefore there is no 100% security* (respondent 8). In this regard, the respondent said that *no significant things happened regarding cybersecurity* which was perceived as a positive outcome, because it might be that they are doing enough. The interview subject specified that within their organisation they make an analysis of the future to assess the chances *of a big cybersecurity incident and how do I make sure that they did enough.* Consequently, according to this respondent being repellent enough towards cyber-risks comes as a result of the resources in place

towards cyber, the risk analysis made as well as whether or not you did enough regarding risks encountered and major attacks perceived, therefore whether the measures that you had in place suited the problems encountered.

When discussing this topic and the measures taken by organisations, some respondents also mentioned the risk-based approach. In this study, the risk-based approach is seen as a precondition for all the procedural and enforcement effectiveness factors to actually occur in practice as it was exposed in Chapter 2. However, some of the ideas shared are relevant regarding being repellent enough to cyber-risks, because some respondents understand it as a cultural thing within the organisations. Respondent 1 stipulated that they promote a risk-based approach and have the proactive culture, the process *goes all the way from the top to the bottom on the operational level*, it is both a cultural thing and about organisational controls to have your risk-management in order (respondent 1). This respondent also said that this is a case-by-case basis and that there is no 'mathematical' method followed.

According to another respondent, the risk-based approach is as follows: *there is an investigation at first and then certification on ISO 27001 only after an incident has occurred and when they have to report or not, so we are happy if they report the incidents* (respondent 4). Other respondents specified that within their organisation they are working on how to manage those risks and be helpful for entities that might encounter problems within their systems (respondent 6). In addition, respondent 8 also focused on the risk-based approach, by specifying how within their organisation the risk analysis was made to repel cyber-risks in the short, medium, and long run.

Overall, our findings are as follows: information sharing, as well as the share of policies, guidelines, and practices being done in organisations alike, might be helpful to be repellent enough to cyber-risks. Also, raising awareness and making the whole organisation and not only the cybersecurity departments aware of the risks online. In addition, using resources to fulfill the needs regarding the risks encountered is relevant in the whole process. Of course, there is always something to improve in cyber and it is difficult to be up-to-date at all times, but risk analysis is key. Finally, ISO and NIST standards seem to be at the forefront, as well as supervisory authorities checking whether or not the measures are in place.

c. Resources to fulfill the objectives

It has been discussed during the interviews that having resources to fulfil cybersecurity risk-management measures are needed. However, some organisations have more resources than others, meaning that depending on when you are talking to a private or a public organisation, a small/medium-sized company, or a multinational with offices worldwide, the resources allocated to cybersecurity might differ.

Generally speaking, the respondents did not emphasise their resources to fulfill their objectives. However, the resources used were embedded in their cybersecurity risk-management framework as well as their ISMS or policies and measures implemented within their organisation. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic.

Firstly, respondent 1 specified that in order to make activities connected to reality, best practices implemented were considered already a first step within other entities, therefore they specified that sometimes the resources used depend on a tailor-made approach, what is already a best practice in the sector is ISO 27001. Similar to this point, respondent 4 also emphasised standards such as ISO and NIST and the need for a tailor-made approach for each sector.

In this line, respondent 2 specified that the size of the company has an effect on this issue, meaning that *smaller companies might leave cyber up to the last moment and they probably hire organisations that tell them what to do to be compliant with NIS2 Directive* (in case they fall under its scope). *Respondents* 3, 5, and 6 did not touch upon the resources needed, only about the scope broadening and the consequences that this might have in the future, without specifying what, but meaning the consequences would be notable. Also, respondent 6 specified that the lack of resources can have an impact on the effectiveness of the activities conducted to tackle risks/vulnerabilities and on developing guidelines, policies, or other means.

In addition, respondent 4 said that within *his organisation investments have been made and a new cybersecurity department has been launched*, therefore the idea behind this is

that the resources taken allow ensuring *that more organisations in their domain have their safety in order.* Finally, this respondent focused on ENISA's lack of resources for which more means are needed to be able to achieve a common report rather than 27 different reports.

According to respondent 7, the resources used in cybersecurity have something to do with harmonising all the time within the Cooperation Group and other networks. Also, this respondent emphasised the following: the risk-based approach should be proportionate because you cannot expect the same *from a medium company in a sector that has maybe limited intellectual property and limited resources* than the capabilities *of a big multinational* (respondent 7). Therefore, resources as well as the size of a company need to be considered when asking for certain maturity levels from Dutch governmental institutions. Moreover, harmonisation is key when dealing with measures taken at both national and EU level organisations, because if the ultimate goal is to reach a high common level of cybersecurity, harmonisation is key as well as other preconditions and factors already showcased in this research work.

Lastly, according to respondent 8, *if we want to be successful digitally, we need to spend enough attention, time, and resources on cybersecurity*. *We have to invest a lot in cybersecurity.* Consequently, according to this respondent, the number of resources destined for cybersecurity allows for better maturity levels within the organisations, while improving the awareness not only in the cybersecurity department but in all the departments within their organisation.

Overall, the main findings are as follows. The number of resources destined to cybersecurity improve the cybersecurity maturity and the measures that allow for reducing the number of potential risks. Therefore, this allows for an effective implementation of the NIS2 Directive in the Netherlands, since the number of risks would be minimised, leading to a distinct approach in handling this topic compared to the NIS Directive. Moreover, the size of the company and the resources at its disposal also have a consequence on the cybersecurity approach and maturity levels taken, for which according to certain respondents small/medium-sized companies and multinationals are not the same and cannot be compared regarding their maturity levels. In this regard, this might have future implications for potential sector-specific legislations since sectors and

organisation's sizes matter regarding the resources destined for cybersecurity risk-management measures. All in all, resources need to be destined for cybersecurity risk-management measures to be able to tackle vulnerabilities and all the departments within entities and organisations need to be on board for this to happen in practice.

d. Lessons learned from the predecessor – the NIS Directive

In this section, the main findings encountered regarding the 'old' and 'new' legal framework are going to be further explained. In the Second NISDUC Conference some analyses were showcased regarding the main challenges of the NIS Directive (see Appendix H). Regarding the obligations of both Directives, these are very similar: duty of care and duty of report, and supervision. This has been further explained in the *'Literature review'* section. However, even though the Directives are quite similar, certain lessons are learned from the NIS Directive. Through the interviews conducted, we found out there are certain lessons learned from the NIS Directive, each respondent gave slightly different approaches, but a general view was seeing in the broadened of the scope as well as the fact that the reporting scheme is positive for the ultimate goal of the NIS2 Directive: high common level of cybersecurity. Now, some specific examples of the respondents' answers will be provided to give light on this specific topic.

Firstly, according to some respondents something that was important with the NIS Directive and will continue to be important with the NIS2 Directive is the cooperation between different competent authoritites, having the end goal in mind. According to respondent 1, they *want to make the most out of it, embedded in* working *effectively to have the most societal effect on what we want to achieve* (respondent 1). Another learning from the NIS to NIS2 Directive is *the scope broadening, because the NIS2 has an all-hazards approach,* also *all network information systems within a company and the physical security of these systems* is been taking into account. *But at the same time securing everything can create some tension from the perception of costs and the societal goal. This is part of the ongoing discussion* (respondent 1). Respondents 2, 4, and 8 also focused on the broadening of scope and how organisations are adapting to it. In this regard, another respondent also focused on the impact of the EU, but also on national legislation of this Directive (respondent 2). In this line, another respondent focused on the fines that are formalised by the Member States (respondent 4). This respondent also

emphasised *cross-border cooperation* (when it comes to supervision), *also who is first to conduct the investigation, and what could be left out. Some things such as risk-assessments and* the way being conducted *are left to the Member States* (respondent 4). Therefore, the approaches to risk analysis and the broadening of scope have been taken into consideration when analysing the shortcomings or changes between both Directives.

Secondly, other respondents focused on both harmonisation and cybersecurity. *Harmonisation held a lot of interpretation room stations and space stations for these two laws* regarding *regulatory bodies* (respondent 3). The interview subjects specify that now cybersecurity is not only for the ICT department but for all the organisation, because of the liability with the new Directive. In this line, respondent 6, the NIS2 Directive aims to address the issue of harmonisation by improving the identification process for entities and facilitating a more streamlined and consistent approach among them. It seeks to establish enhanced baseline security requirements for these critical entities. Essentially, it strives to enhance upon the shortcomings of the first Directive by introducing elements like CVD policies, the EU vulnerability database, and the inclusion of additional sectors deemed crucial for the economy (respondent 6). Therefore, the NIS2 tries to further explained the elements that the first Directive fails to do.

Thirdly, another respondent said that NIS2 broadens the scope and adds administrative bureaucracy and that *NIS2 brings more rules, but the rules are needed to solve issues faster* (respondent 5). Also, according to respondent 7 *notification obligations, throughout Europe* proves to be a challenging task. Setting the thresholds too high results in a lack of notifications, while setting them too low leads to an overwhelming influx of notifications that may not necessarily contribute to the effectiveness of one's work (respondent 7). This respondent said that this will continue to be a challenge with the new Directive. *If you look at the impact assessment of this tool, you see a lot of these challenges that we have also faced with building the relations between the supervisory authorities and the companies* (respondent 7). Also, he said that *with NIS one, it was still feasible to really focus on personal relationships. So in NIS one, you saw a lot of voluntary notifications and information sharing, which is really helpful* (respondent 7). Therefore, according to this respondent broadening the scope has as a first consequence that the development of personal relationships gets complicated, meaning that a trustworthy network is more difficult to achieve, but not impossible.

So far, the preconditions of risk-based approach, harmonisation, as well as trust, have popped up when dealing with lessons learned or shortcomings of the NIS Directive.

Finally, according to respondent 8 a challenge of the legislation is *how to show compliance* because *that is where things go into detail, where the opinions differ, and where you need to have very specific knowledge.* The challenge for this respondent is to translate the high-level legislation into control measures and objectives in practice which might be a challenge for the implementation of the Directive in the Netherlands if agreements are not happening.

Overall, the points made by respondents differ to a certain extent. However, one of the main findings was that the broadening of the scope of the Directive is double-edged. First, it allows for more organisations to have their measures up-to-date and achieve the ultimate goal of the Directive jointly. While, it creates a problem regarding harmonisation and trust between the institutions, because just in the Netherlands the number of organisations increased from a couple of hundred to thousands, thus knowing all the people involved in the process might be more difficult nationally, but this also increases the difficulty regarding cross-border cooperation. To a lesser extent, the point made by some respondents is that with NIS2 Directive some policies and guidelines are more developed and more concrete than with NIS Directive, but this is high-level legislation and it might be a challenge to specify the control objectives and measures that organisations need to take into account. Therefore, the implementation of the Directive into national law is expected by the respondents to solve certain issues along the way. However, the extent to which this implementation will solve all challenges is yet to be seen.

e. Uniformity

In this study, uniformity is understood at the national level. Therefore, to what extent the Dutch government is implementing measures and approaches that are uniformly implemented through the different sectoral ministries of high criticality and the governmental institutions in general. In the interviews conducted, the term uniformity, coordination, and harmonisation has been used indistinctively. This might create an overlap with one factor of the *'Procedural effectiveness'* section which is *'Coordination*

nationally'. However, in this study the consideration of the uniformity factor comes as a result of whether or not there is coordination and harmonisation within the governmental institutions as it was discussed in Chapter 2 when describing the precondition 'harmonisation', and to a lesser extent the harmonisation within public and private sector's approaches (more the semi-private organisations).

It is relevant to go through the *'Coordination nationally'* factor and some remarks made by the respondents, because this will show certain specifics that are necessary to be taken into account. Now, some specific examples of the respondent's answers will be provided to give light on this specific topic. A relevant point made by respondent 1 is that *on a methodology level, you have the same framework, but the way of translating it to your intervention strategy can differ between organisations. So even with the same law, the same measures, the same activities, and how you actually do this might differ between the organisations and the way we act on it* (respondent 1). Consequently, a main inference is that cooperation is aimed for, but in practice, the way the structure works makes the aim difficult to achieve. There is a collective effort through different meetings to harmonise approaches, but in the end, each organisation needs to fulfill this. Therefore, uniformity is aimed at the Dutch governmental level, but in practice, the structure of the government has consequences on how to proceed with the uniformity of their approaches and this can be hampered due to being formed by different bodies implementing slightly different measures.

Secondly, another point made is regarding the coordination nationally being done by NCTV's role. Moreover, respondent 3 said that their *organisation has tight working relations with other departments, e.g., the Department of Economic Affairs, departments for General Affairs, and for Defense. We have to coordinate with the target groups that are vital organisations and Dutch central government, and the vital organisation are in the care of the Ministry of Internal Affairs and the Dutch government.* This respondent emphasised that harmonisation is key in the NIS2 Directive when comparing it with the NIS Directive.

In light of the above, another respondent also focused on the fact that harmonisation in the Netherlands is key. This respondent said *that there are a lot of meetings to benchmark our efforts and share information* with *the regulatory bodies.* Moreover, the respondent

said that *the different departments are meeting regularly to develop interdepartmental collaboration for policy and for inspectorates* (respondent 4). In light of the above, the meetings allow for harmonisation in the measures implemented by the different sectoral ministries, which implies that the first steps towards uniformity are being made. However, the fact that the NIS2 Directive is yet not transposed into national law has been exposed as a deterrent and the effects this might have on the Netherlands will be further analysed in the near future.

Lastly, two respondents emphasised the room for interpretation of the NIS2 Directive (respondents 7 and 8). This room for interpretation has consequences not only at the EU level, but also at the national level. Because in this regard, a recurrent topic in the interviews was whether or not sectoral acts are needed, some agreed and one respondent disagreed. Moreover, it has been inferred by several respondents (1, 3, 4, 5, and 7) that the main coordinator is the NCTV. One interviewee said that during the *whole process they have coordinated in an inter-ministerial way between the agencies making sure their output publications before the NIS2 Directive were published, and well represented* (respondent 7). This respondent emphasised that with the new national cybersecurity strategy, the idea in the Netherlands is to go to a more centralised approach, because now it is rather decentralised. Consequently, it can be argued that with NIS2 Directive the idea is to make uniform the governmental approach towards cybersecurity risk-management measures with the ultimate goal in mind: a high common level of cybersecurity.

The coordinated inspection framework of cybersecurity of critical processes shows that three out of six supervisory bodies in total have organised their supervision of cybersecurity on a solid basis, while other supervisory bodies are still working on this (CSAN, 2022, p. 28). In this regard, supervisory activities are relevant in the process of harmonisation and uniformity of the measures in place in the Netherlands, since all of the supervisory authorities are part of the same body: the Dutch government.

Overall, it seems that uniformity, harmonisation and coordination are factors taken into account by Dutch organisations (either from the government, private, public, or semi). However, it can be inferred that this uniformity process is ongoing, therefore the results would need to be analysed in the future once the NIS2 Directive is transposed into national law in the Netherlands. It can also be argued that Dutch institutions are already

working on this centralisation and harmonisation of approaches and as a result, frequent meetings, ISO/NIST standards as well as horizontal information-sharing schemes are in place to a certain extent. Another finding is that quite often harmonisation, trust and information sharing are interrelated, without one of them is difficult to reach the others. Therefore, it could be argued that uniformity comes as an outcome when dealing with procedural and enforcement effectiveness factors.

Chapter 6. Outome of the research

When doing the literature review, conducting the interviews, and attending different conferences in April and May, one of the main outcomes was that the implementation of the NIS2 Directive is still in its infancy in the Netherlands. Almost all respondents referred to the NIS Directive rather than the NIS2 because the latter is still in needs to be transposed into national law, the national law for the NIS Directive is the Wbni (2018) as it is further explained in Chapter 4.

This implied that the findings differ regarding the actual implementation of the cybersecurity risk-management measures going more towards the direction of collaborative processes of general awareness as well as the spill of knowledge among the different institutions and organisations involved. These organisations are not only from the government or EU level but also from the industry. Regardless, the outcome of this research has been fruitful, since several main findings have been encountered.

Firstly, the entry into force of a Directive does not equal the starting of implementing the measures in a country, since the transposition into national law of this Directive is being considered key for all the respondents. Furthermore, international standards such as ISO and NIST are seen in cybersecurity as a basis and a first step to implementing a cyber-secure policy within public and private organisations of different kinds, notwithstanding their size cap.

In addition, this research serves to analyse that the EU level is generally detached from what happens in practice regarding cybersecurity, meaning that it has been encountered that usually, people consider the legal framework broad and difficult to follow, with the need for sector-specific legislation, while at the EU level, the focus is in other legal

proposals for similar issues that can potentially see an overlap with the already existed legislation. Consequently, a lack of concrete definitions for a shared problem can be regarded as a challenge, as demonstrated in this study regarding the definition of a cybersecurity risk-management framework and measures, as well as the variations in approaches among the interviewed organisations/entities/companies.

It has been perceived that the factors of cooperation, collaboration, and information sharing are interrelated in practice with the preconditions of trust and harmonisation mainly. Firstly, trust within the network is essential for organisations at both the national and EU level to collaborate and share information with each other. This leads to another outcome, which is the harmonisation of the measures implemented. Because without trust in the network, harmonisation and thus uniformity can be hampered and, therefore the ultimate goal of the Directive 'high common level of cybersecurity' is difficult to fulfill in the Netherlands.
These factors, without these preconditions, do not lead to procedural and enforcement effectiveness in the Netherlands. Meaning that without a trustworthy network, organisations are less willing to share information regarding incidents as well as the fact that not having a trustworthy network might imply that the information is not shared and that therefore fines might come. Cybersecurity knows no borders and we are going towards a more digitalised society, for which clear norms and codes of conduct are needed; as well as harmonised approaches in the way the government proceeds with the measures at stake. Otherwise, the effectiveness of the measures could be hampered in the Netherlands.

In light of the above, this research tried to analyse, assess and answer the research questions exposed in Chapter 1. In this regard, first this research work will zoom in the sub-research questions to be able to answer the main research questions.
After all the data gathering process has been finalised, the definition of cybersecurity risk-management framework is rather blurred in the Netherlands as well as the cybersecurity risk-management measures. This is the case, because it has been argued that the NIS2 Directive still needs to be transposed into national law and once this happens specific definitions will be provided and even sector-specific clarifications might be needed. However, it seems that waiting for the transposition into national law to solve this problem with definition might be too enthusiastic and this leads to solve this problem in

the future. Therefore, according to the findings of this research, cybersecurity risk-management measures need to be technical, operational and organisational, that everyone within the organisation needs to understand the consequences of risks and incidents in ICT systems. Moreover, risk-assessment and risk analysis need to be done by the organisations under the scope of this Directive, bearing in mind that there is no 100% of security and there is always a need of being updated.

Secondly, regarding the supervisory activities by the competent authorities in the Netherlands, this supervision needs to be done plus the compliance with international standards such as ISO or NIST. These standards are the most widely used within the industry and public administration sectors. The supervisory authorities follow a process when it comes to monitoring the measures taken by entities, but the resources and maturity levels of these entities need to be taken into consideration in the process. Therefore, the monitoring of the activities of entities under the supervision of the competent authorities does not follow a mathematical approach, instead, it depends on a case-to-case basis. For this, the ISO 27k series is considered a good first step for those entities whose maturity levels are rather in their infancy.

In addition, regarding the differences and similarities encountered in the approaches taken by the Dutch governmental institutions, the findings are two-fold. First, the Dutch government works as one but is formed by different bodies and each of them has slightly different approaches to cybersecurity risk-management. Secondly, the sectoral ministries have a relevant role regarding the implementation of the NIS2 Directive in the Netherlands. Within these ministries, monthly meetings are happening to harmonise approaches towards cybersecurity risk-management measures. However, this harmonisation is still in its infancy. It is also important to take into consideration, that coordination and collaboration within a huge network nationally requires of a combined effort with a common goal in mind: cybersecurity. If this is already a challenge at the national level, at the EU level it gets even more complicated. Therefore, the process of harmonisation and uniformity of the measures at the national level needs from information-sharing schemes, trustworthy networks, cooperation, and collaboration (nationally, cross-border, and public-private sector); it also requires from organisations to being repellent to cyber-risks, following a risk-based approach and compliance, among others.

Finally, this leads to whether and to what extent the Dutch governmental institutions uniformly implement the Directive's cybersecurity risk-management measures. In this regard, uniformity is an outcome aimed for, but much more needs to be done in practice for this to happen. The NIS2 Directive is not been transposed into national law yet, but efforts need to be done towards a harmonised and uniformed approach regarding these measures because this would allow for an effective approach to cybersecurity risk-management framework in the Netherlands. For this to happen, the factors taken into consideration in this research for both procedural and enforcement effectiveness need to be fulfilled as well as the preconditions analysed in Chapter 2. However, in the case of the Netherlands, it is halfway through to fulfilling this effectiveness framework.

Overall, this allows us to answer the main research question that has shaped this research from beginning to end. The approach followed by the Dutch governmental institutions is a decentralised one, meaning that each sector depends on its sectoral ministries and sectoral supervisory authorities. Efforts are being undertaken towards a harmonised approach, but this is still in its infancy. The Netherlands is halfway through fulfilling both procedural and enforcement effectiveness regarding the implementation of the NIS2 Directive. This is the case because even though the Directive is not transposed into national law, the NIS Directive has already been transposed through the Wbni. Then the steps followed by entities are not changing too much from both Directives, of course lessons have been learned with respect to the NIS Directive. But waiting for the transposition into national law might be too late for this implementation to be effective in the case of the Netherlands and it might be that sectoral clarifications are needed to make it even more effective in the near future. Therefore, there is room for improvement regarding the principles, factors, and preconditions analysed in this research work. Broadly speaking, more collaboration vertically is needed. The public enforcement bodies can be benefitted by the resources and maturity levels of the private sector and trust leads to information-sharing schemes (both horizontally and vertically).

6.1. Policy recommendations

Considering the above, this study has come up with several policy recommendations that try to depict the challenges encountered in the data gathering process, while trying to bring light to the future transposition of the NIS2 Directive into national law in the Dutch case. The aim is to provide policy recommendations that target governmental organisations in the Netherlands, but also the private sector and even EU institutions that are involved in the process either through the NIS Cooperation Group or in other networks throughout the process.

In this section, actions covered by the National Cybersecurity Strategy and ISO standards will be taken into consideration, this is the case because it is considered that this might have a better practical impact, which allows for actual improvements in practice in the medium and long term. Even though the Directive has not been transposed into national law, understanding what actions to take is crucial in determining the potential effects of the transposition. Because otherwise, this will not have practical consequences and because it is fundamental to be always ready in cybersecurity since technology is constantly changing. Therefore, the more preparation, the better.

1. **The Directive should not leave leeway on the measures to implement.**

The nature of a Directive leaves leeway to Member States to implement the Directive regarding their own resources and procedures. However, in this case, such leeway is considered rather negative in practice. This is the case because certain common definitions such as cybersecurity risk-management or framework are left to Member States to decide what measures, timings, and other practicalities to decide. However, this leads to a constant debate on whether sector-specific decrees are needed at EU or national level as well as the differences in resources among Member States. Therefore, the EU negotiations on the Directive should come up with certain basics in the form of a Regulation, since the main common goal is a high common level of cybersecurity. For which common definitions of common problems are needed.

Therefore, the EU should stipulate as a Regulation Chapter IV of the NIS2 Directive 'Cybersecurity risk-management measures and reporting obligations.' Consequently, harmonised approaches would be binding to all Member States in the same way. This is needed because harmonised approaches would be aimed at the

implementation of the Directive and future Regulations in the Netherlands on the topic.

2. **Cybersecurity risk-management measures need to be harmonised and sector-specific in the Netherlands.**

Firstly, the measures need to be harmonised. As in pillar one of the Dutch strategy 2022-2028 'Cyber resilience of the government, business, and civil society organisations', one of the main aims is for the governmental organisations, such as CSIRTs and supervisory authorities, to share information effectively, nationally, and internationally (NCTV, 2022, p. 25). This needs to be done because otherwise there are different measures implemented scattered in the same system. In this line, coordinated and integrated risk is still in its infancy (CSAN, 2022, p. 28). Also, following the cybersecurity strategy, consistency in terminology nationally on the resilience of critical entities (NCTV, 2022, p. 26), as well as harmonisation on the implementation of European and national legislation in the Netherlands is aimed for (NCTV, 2022, p. 27). **Therefore, the Dutch government with the Ministry of Justice and Security needs to harmonise the measures at the national level. Hence, the Dutch system works with the same parameters, since the core goal is the development of a mature approach of risk-management at organisational, sectoral, and national level, but the fact that there are a number of different risk analysis methods hampers internal and cross-organisational discussions about risk-mitigation and acceptance in light of the CSAN report (2022).**

Secondly, there is a need for a sector-specific approach to the measures. Because according to pillar 1 of the aforementioned strategy, some sectors are also subject to additional legislation that imposes sector-specific cybersecurity requirements at least as stringent as those set out in the NIS2. The sectoral ministries are responsible for drawing up this sector-specific legislation and the Ministry of Justice and Security ensures that European and national legislation relating to cybersecurity is developed and implemented in a harmonised manner (NCTV, 2022, p. 27). **Therefore, the Dutch governmental institutions need to work on sector-specific decrees, since each sector has characteristics that cannot be correlated with other sectors.**

Finally, national, European, and international standards might help in the process. However, standards are not laws, but they allow to show that a product or a service within an organisation either public or private, meets certain requirements. In the Netherlands, different types of standards are in place: national standards such as NEN, European standards such as CEN and CENELEC or ETSI, or international standards such as ISO/NIST (RVO, 2022). This study has considered ISO and NIST standards because they are widely known and, in the sectors involved, international standards are widely used. However, some national standards could bring light to the measures to implement as well. Among the standards this study considers key to use in the Netherlands and that are already in use in practice worldwide, are: i) **ISO/IEC 27001:2013**, information security, cybersecurity, and privacy protection. Information security management systems. Requirements; ii) **ISO/IEC 27005:2011**, information technology - Security techniques – information security risk management; iii) **ISO/IEC 29147:2014**, information technology. Security techniques. Vulnerability disclosure. Gives guidelines for disclosure of potential vulnerabilities in products and online services; iv) **ISO 31000:2018,** risk management – Guidelines; v) **NIST 800-300** in which definitions and the practical guidance required for assessing and mitigating risks identified with IT systems (ENISA, 2018, pp. 55,56).

It is important to note though that a standard cannot be used as a strategy and that being certified by the aforementioned organisations does not mean that you are 100% secure. However, these standards serve as a basis for having your risk profile up-to-date. For instance, both internal and external audits are key in this regard. In the Second NISDUC Conference (2023), speakers talked about an internal audit every year and an external audit every three years. **Maybe both an internal and an external audit every year would incentivise organisations more to have their systems updated, and so all departments within the organisation are aware of cyber as well.**

Of course, it cannot be denied that the establishment and management of a security supervision framework in the context of the NIS Directive involves challenges such as the lack of resources and the rapid change of technology and standards. Nevertheless, the effective utilisation of the audit output is essential to the evaluation of the implementation of required controls on both the technical and operational levels (ENISA, 2018, p. 29). In some reports by ENISA (2022, p. 132), these are the recommendations taken into account.

Consequently, this can have positive impact in practice. Because as a result of the audit, it comes a report outlining the observations and/or recommendations depending on a case-by-case basis. Moreover, the implementation of a roadmap for the organisation to follow, with proposed corrective actions and an implementation timeframe (ENISA, 2018, p. 29). **Cybersecurity procedures are always ongoing, therefore measures need to be updated across all sectors in the Netherlands, notwithstanding the size and resources of the organisations under supervision. This will benefit the implementation of the NIS2 Directive into national law in the Dutch case, because it will allow for harmonised measures similar for all, as well as stipulating for each sector measures that pinpoint on specific challenges encountered.**

3. More collaboration and harmonisation both horizontally and vertically is needed.

3.1. Harmonisation

Following up on the harmonisation of measures in the Netherlands, harmonisation and collaboration both horizontally (governmental institutions-governmental institutions) and vertically (governmental institutions-industry) are needed. This study considers that information-sharing schemes, as well as trustworthy networks among sets of organisations might benefit the collaboration and harmonisation of cybersecurity in general in the Netherlands. Moreover, it adds to the aim set in the national cybersecurity strategy as well.

Consequently**, the organisation of workshops, conferences, or intersectoral meetings on a regular basis might help to reach good levels of trustworthy relationships while adding to the harmonised approach to cybersecurity. Public-private partnerships are something to aim for to be cyber-resilient. This benefits the Dutch implementation of the Directive, because it learns and coordinates approaches that are needed to reach the ultimate goal of the Directive in the country.**

3.2. Trustworthy network

It is important to create a trustworthy network, not only at the governmental level, but also through public-private partnerships because the private sector has the resources while small and medium-sized companies need those resources and knowledge to higher-up their maturity levels.

Reaching trust within the network allows to foster information sharing by i) improving capabilities and detection engineering; and ii) spill of knowledge through guidelines, reports, and/or policies. Therefore, information and best practices are needed to improve positions towards cyber. This goes in line with what has already been agreed on in the cybersecurity strategy: i) cyber incidents affecting business and public authorities could lead to a loss of consumer confidence or of public trust in the government (NCTV, 2022, p. 24); ii) central government provides a stimulus for greater and more effective collaboration between organisations, to ensure that cyber-capabilities are deployed as effectively and efficiently as possible (NCTV, 2022, p. 28); and, iii) organisations will need to be more proactive in sharing their experiences and lessons learned with each other, for which trust is crucial (NCTV, 2022, p. 28).

This can be hampered by the fact that Dutch infrastructure could be exploited, or it could be affected by possible counteractions, such as the disconnection of digital infrastructure by countries hit by a digital attack (CSAN, 2022, p. 23). **Therefore, the Dutch government needs to create a trustworthy network in which public-private partnerships are at the front. Trust within the system is key to provide with information-sharing schemes. With trustworthy networks and information-sharing schemes, the implementation of the NIS2 Directive can be beneficial, because this allows for the system to repel cyber-risks or reduce its number while harmonising approaches and reaching the high common level of cybersecurity aimed at the first place.**

4. Need for interdisciplinary experts in both law and cybersecurity risk-management

Following-up on the pillar 4 of the national strategy ‘Cybersecurity labour market, education and cyber resilience of the public’, regarding the aim on the Dutch labour market to meet the growing demand for cybersecurity experts (NCTV, 2022, p. 42). This study considers that more experts in both EU law and cybersecurity risk-management are needed. Organisations in the Netherlands offer to upskill and reskill programmes for cybersecurity expertise. Therefore, more law and cybersecurity experts are needed, because differences between Directives and Regulations need to be understood in practice, while the differences between ISO, NIST, or NEN standards as well as the differences between mitigation and evaluation or the different controls used by organisations need to be clearly understood. **Therefore, by having interdisciplinary**

experts on this issue a general understanding of the difficulties in the process might be properly fulfilled. This interdisciplinary background can be achieved by organising bachelor or masters' programmes that combine computer science and law, as well as the organisation of conferences, workshops, or seminars on the topic on a regular basis and free of charge. Making people both aware and interested in these topics is the first step towards an interdisciplinary approach of cybersecurity in the Netherlands.

Moreover, this impacts the risks perceived, because high risks come from not acknowledging online activities, such as email usage, online shopping, and everyday tasks online. Therefore, experts on both law and cybersecurity are needed so the transposition of the Directive into national law would be more nuanced and goal-oriented.

Chapter 7. Conclusions

This study aimed to address the following questions: *What is the approach followed by the Dutch government to ensure compliance with the NIS2 Directive and how does this contribute to the effectiveness of cybersecurity risk-management measures in the Netherlands? To what extent is there room for improvement, in light of the principles of procedural and enforcement effectiveness?* This paper combines qualitative mixed methods to gather information supporting our arguments to bring light on the Dutch critical infrastructure approach to cybersecurity risk-management framework and measures in light of the NIS2 Directive.

This study has been based on the theoretical framework of procedural and enforcement effectiveness, which allows zooming in on the practical impact of EU Directives, by not only analysing the level of autonomy, decision-making, and cooperation processes of the policy at stake and between the actors involved (procedural effectiveness) regarding the NIS2 Directive, but also the effect that organisations such as the Dutch governmental institutions have on the sectors of high criticality when it comes to change measures over time due to new legislation such as the NIS2 Directive by being liable, repellent to cyber-risks among others (enforcement effectiveness). Thus, procedural and enforcement effectiveness are interrelated, one comes as the consequence of the other. The different

factors for each type of effectiveness have been already analysed, but it is important to keep in mind the main findings here.

Firstly, information-sharing schemes happen within the network of governmental institutions or within the network of private entities. However, when it comes to the information sharing between governments with entities, the trust levels seem to lower or the information sharing only happens regarding the threshold agreed by law, but no more.

Secondly, the Dutch government is formed by different bodies, therefore coordination and harmonisation of the measures in place might be difficult to reach. Nevertheless, it seems that when it comes to the sectoral ministries, the communication between these ministries and the industry is ongoing and it is relevant. In practice, it seems that coordination is happening, but it really depends on to whom you are talking to, the sector they are part of, and the resources they have at their command, to see the approach they take towards coordination, collaboration, harmonisation, and if they agree on this happening in practice.

Thirdly, depending on the organisation, cross-border cooperation is seen differently, meaning that in certain cases cross-border cooperation happens just by talking with everyone, while for other respondents cross-border cooperation is the result of sectoral work streams working together to harmonise their approaches when dealing with risks and incidents on a daily basis. All in all, the Netherlands seems a country quite invested in the topic of cybersecurity, therefore all resources and energies are channeled towards it, but more effort needs to be made to keep everyone aware of what happens in practice.

Moreover, public-private cooperation is still in its infancy in the Netherlands because the extent to which this happens is still under debate. This is happening not only in the Netherlands, but across Europe. However, at the EU level networks such as the CSIRTs, NIS Cooperation Group, or EU bodies for each sector or industry are in place and dialogue is happening, maybe even more than within national systems per se. Moreover, these partnerships are relevant and need to work, because the public sector could be highly benefited from the knowledge and resources of the private sector.

In addition, the ongoing debate of risk-based vs. compliance approach needs to be further analysed once the NIS2 Directive is transposed into national law. But one main takeaway seems clear: being certified does not mean being secure and as an entity, you follow a risk-based approach and once you have come up with it, supervisory authorities check your compliance. Moreover, both approaches are considered a precondition in this study, because being repellent to cyber-risks comes as a factor. However, these concepts have been used indistinctively in interviews and conferences attended, therefore more analysis needs to be done. Moreover, the conclusion is two-fold: compliance with ISO or NIST standards is enough in certain cases in which the maturity levels are not so high (e.g., small/medium-sized companies); and, secondly, compliance with these standards without supervisory activities and constant up-to-date measures do not work. Because there is no 100% of security, all the efforts need to be destined to achieve certain levels of security and thus maturity. If the main goal is a high common level of cybersecurity, efforts need to be put into repelling risks, having up-to-date measures, and doing risk analysis, assessments, and mitigation plans.

Furthermore, uniformity in the Dutch approach to cybersecurity risk-management comes as a direct consequence of whether or not the Dutch government is sharing the information within their departments, collaborating with partners in both public and private sectors, as well as coordinating procedures. In this regard, the CSAN report (2022) shows a huge effort by the supervisory authorities to harmonise approaches, but more should be done according to the data presented in this study and in the report. Consequently, harmonisation, trust, and information sharing are interrelated, without one of them is difficult to reach the other and all of them allow for a process of uniformity in the Dutch governmental institutions. Therefore, uniformity cannot be reached if the other factors of *procedural effectiveness* are not in place in the Netherlands.

Additionally, personal and institutional liability seems a double-edged measure to implement, because while it is seen by some as an incentive to have cybersecurity risk-management framework updated, it is also seen as making organisations less transparent and willing to share the information with other organisations. While doing a cost-benefit analysis of whether paying the fines or being secure as an either-or position, to assess what is more suitable option for them. Therefore, other measures might be into place to

avoid this situation, but these fines cannot come as a surprise to the entities, there is a rather long process beforehand.

Besides, resources need to be destined for a cybersecurity risk-management framework to tackle vulnerabilities, since these resources help to improve the maturity levels of organisations of different natures, while it allows retaining potential risks. Therefore, other organisations are benefitted since the levels of digitalisation of everyday activities are increasing over time.

Also, trustworthy networks are key both horizontally and vertically. Trust is considered a precondition in this study, therefore trustworthy networks are necessary so the information-sharing schemes happen in practice both at the EU and national levels. Moreover, the more trust is gained, the better the results might be, because this trust comes with: i) a share of knowledge, ii) a share of the number of incidents, iii) 'successful' best practices, and so on. In this regard, interpersonal relationships and networking seem key, but with the broadening of the scope of the Directive, this might be difficult.

Lastly, the broadening of the scope of the NIS2 respected of the NIS Directive is double-edged. Firstly, it allows for more organisations to have their measures up-to-date and achieve the goal of the Directive jointly. While it creates a problem regarding harmonisation and trust between the institutions because just in the Netherlands the number of organisations increased from a couple of hundred to thousands. To a lesser extent, with the NIS2 Directive some policies and guidelines are more developed and concrete than with the NIS Directive, which sheds light on the organisations under the scope of NIS2.

It can be therefore said that the Netherlands is halfway through reaching the procedural and enforcement effectiveness regarding the cybersecurity risk-managament framework in light of the NIS2 Directive. Three things seem key in order for this to happen: information sharing and CVD policies, trust within the network, and collaboration both horizontally and vertically. Moreover, without the preconditions analysed in this study: harmonisation, risk-based approach, compliance, and trust, the result might not be optimal.

On the other hand, the interviews with both 'regulators' and 'consumers' of the legislation in the Netherlands, but also EU institutions related to this issue have been key. Each of them gave slightly different approaches to the same topic: cybersecurity risk-management framework and measures. The differences were regarding the introduction of the Directive, the nature of the Directive, and the fact that leaves leeway to the Member States to implement the measures by sector-specific acts and whether or not this could be done in the future.

Several factors and actors are involved in cybersecurity. Therefore, several factors explain Dutch governmental organisations' perception of cybersecurity risk-management measures. These factors have been explained already, however, it is important to emphasise that information sharing, coordination, cooperation, liability, uniformity, repellent to cyber-risks or lessons learned from the predecessor - NIS Directive, have an impact on the approach of the eight respondents towards EU legislation with the ultimate goal of a 'high common level of cybersecurity'. By and large, Dutch industry and government are highly aware of the role of EU institutions in shaping a safe and secure cyberspace and specific national, European, and international standards for this to happen. However, the size and resources of organisations might have an impact on whether the maturity levels reach certain thresholds.

Firstly, the organisations are still finalising the implementation of the NIS Directive, therefore the NIS2 Directive is still in its infancy regarding the measures to be implemented and the NIS2 Directive needs to be transposed into national law. Once this happens, it will become apparent whether there is a requirement for sector-specific legislation in the Netherlands or not. Secondly, the lack of a common definition for cybersecurity risk-management framework and measures in the Directive even though the concept appeared throughout the document has negative consequences, because it does not allow for harmonisation on the approaches taken by both government and private sector organisations. Therefore, it might hamper the approach to cybersecurity in the Netherlands and in the EU. Thirdly, sector-specific legislation or centralisation at the EU level is needed, at least when it comes to reporting to EU institutions, centralisation in agencies such as ENISA might be beneficial, because then there would be one report instead of 27 different reports nationally. In addition, information sharing is key in this issue, because the private sector has the resources and the public authorities the executive direction for the organisations to implement the measures. Moreover, without a

trustworthy network both horizontally and vertically, no results will be achieved. This is the case because networks need to be trusted within the governmental institutions and the industry separately, but also among both groups jointly.

Furthermore, certain overlaps are been seeing within new EU legislation which complicates further the guidelines that need to be followed, for which governmental institutions as well as the industry might need more trainings in order for them to be able to understand these issues better.
With the NIS2 Directive the scope of entities is broadened and more insitutions take part on the ultimate goal shaped by the Directive. However, even though more explanation is added, there is no concrete idea of what cybersecurity risk-management measures are. NIS2 Directive is a high-level legislation and this comes with challenges: i) there is a detachment of the EU institutions from what happens in practice; and ii) there is a lack of experts in both EU law and cybersecurity risk-management. Consequently, people with no background in cybersecurity risk-management are shaping legislation without considering certain specifics of the 'cyber-world'. This comes as a problem because depending on the size of the organisation, the maturity levels or the resources commanded to cyber might differ, and even the NIS2 Directive might come as a repetition of what they have been doing so far or as something completely new that they do not know how to handle. In this regard, throughout the process, ISO and NIST standards are key, because they are internationally accepted and these might be an 'easy' and costly first step for those organisations with lower maturity levels to be driven by a risk-based approach or compliance approach. However, this raises another conclusion which is whether or not being compliant with those standards is enough, debate that is still ongoing in practice.

In this line, the ongoing debate about the approach to take, either a risk-based approach or a compliance approach. These two have been juxtaposed in practice. Consequently, the findings show that being compliant does not mean being secure and that ISO or NIST standards do not equal a strategy for cybersecurity. Other findings stipulate that it is about a 'culture of awareness' within organisations of different kind and how to reach that culture. In addition, supervisory activities are needed to assess whether the risk analysis and risk posture are updated and following the requirements stipulated by law. Apart from this, the duty to report by the entities is relevant. Also as it has been showed sometimes the reporting only happens as an answer to the threshold stipulated by law and the rest of

the information is directed to NCSC-NL. However, the latter has a policy of trust and no disclosure, therefore they need to see how to proceed on a case-by-case basis.

It seems though that this is quite an opaque procedure in which organisations prefer not to disclose information for maybe reputational damage or other main drivers. There is no solution or mathematical approach that could be followed, but it seems that information sharing on incidents and reporting is needed in order to be able to stipulate the correct patches in the system because otherwise the system will not be prepared for certain risks. Of course, another thing to be done is raising awareness within the organisations and the general public as well, since daily life tasks are disclosed online and over time more information is shared in the cloud/Internet/IT and OT devices. However, this needs to be done with precaution since blaming the victims or the people for not being able to understand how the system works should not be the way, this is an ongoing process in which everyone needs to understand the basics such as software updates, multi-factor authentication, delete anything that you do not trust and so on. But in order to be able to do that, guidelines, reports, and policies need to be harmonised not only in the Netherlands but elsewhere. This is a group effort and rather complicated, but we are halfway through in the Netherlands.
There is no such thing as 100% of security, but the more we understand what to do to avoid certain risks is already a lot that has been gained due to Directives such as the NIS2 Directive.

7.1. Limitations of the study

This study has encountered certain limitations that need to be considered in this section after conducting the semi-structured interviews and analysing the results. One limitation is reliability of the study because the total number of interviews is eight. Even though the information provided is fruitful, this study could be further benefitted by more respondents across sectors in the Netherlands, so the sample size is rather small and the results would be empirically more significant if the number of respondents was higher.

Secondly, since the NIS2 Directive is still in the process of being transposed into national law, the respondents centralised their answers on the NIS Directive instead, therefore in some cases in which answers from the NIS2 Directive were not provided, the NIS

Directive is taken into consideration. Consequently, further research on the topic is needed to bring light to this issue once the NIS2 Directive is transposed into national law, which has been postponed to be enforced with the CER Directive jointly.

Thirdly, the scope of the research aimed for at the beginning included also the health sector. However, the scope was narrowed to digital, transport, and public administration because the health sector did not show interest in the research.

In addition, more time on the data gathering process would be needed to be able to analyse the data more comprehensively, because the process of contacting potential respondents started in February, the first interview was scheduled for the 30th of March, and the last one for the 22nd of May. Consequently, time constraints need also to be taken into account in this study.

Lastly, focusing on the theoretical framework of both procedural and enforcement effectiveness can be understood as subjective, since different factors have been taken into consideration, but other factors could potentially have an impact on the respondents' answers and their approach to the implementation of the cybersecurity risk-management framework and measures in the Netherlands. For instance, it might be that organisations take as a factor 'the number of risks' they have encountered rather than any other variable, meaning that by a smaller number of risks the measures are effective and for a bigger number of risks the measures are ineffective. Organisations of different natures may have multiple and heterogeneous measures in place.

7.2. Topics for future research

This study has been centered on the topics of cybersecurity risk-management framework and measures in light of the NIS2 Directive in the case study of the Netherlands. Specific sectors have been taking into consideration, because otherwise the scope will be too broad. However, there are certain topics that have been discussed in both interviews and conferences attended that could be interested to be analysed as part of future research. These topics are as follows. Firstly, the topic of harmonisation has been indistinctively compared with coordination and collaboration both nationally and at the EU level. Therefore, it would be interesting to analyse the harmonisation within

Member States' approach to cybersecurity risk-management through a comparative case study for instance.

Secondly, when dealing with cross-border cooperation and a trustworthy network, the NIS Cooperation Group was mentioned multiple times. Therefore, another topic of interest would be the NIS Cooperation Group and the collaboration schemes among Member States and the industry. In line with this, another topic interesting to analyse would be the CSIRTs network collaboration or the ISACs as well. These collaborative networks go beyond the scope of this research, but are relevant still.

Thirdly, due to the NIS2 Directive not being transposed into national law just yet, it would be interesting to see how the Directive is implemented in the Netherlands but also in other Member States and the process that Member States follow. For instance, during the autumn of 2023, the deliberation within the Dutch government will take place to transpose the NIS2 Directive into national law and entry into force may be at the end of 2024. However, due to time constraints, this research cannot cover this process.

In addition, it has been specified throughout this study, in conferences attended and interviews conducted that the risk-driven approach and the compliance approach differ. Meaning that the main objective is to go towards a more proactive approach when dealing with mitigation plans and risk-management measures in the EU Member States. This field of expertise is booming and future research will be relevant to see the implications in the legal framework across the Union and within the sectors of high criticality.

Lastly, regarding the new sector under the scope of the NIS2 Directive: the public administration sector, and taking into consideration the 'NIS2 legislation for EU institutions' briefly exposed in this study, it would be pertinent to see how they implement the measures and whether or not they follow European or international standards such as ISO/NIST within the EU institutions. In line with the future liability to EU institutions under the scope of the NIS2 Directive, this might have an impact on the Council and the networks relations within the Permanent Representations of countries such as the Netherlands. The role of the latter regarding the implementation of the NIS2 Directive in the Netherlands would also be significant to be analysed as future research.

References

Aberbach, J.D. & Rockman, B.A. (2002). Conducting and Coding Elites Interviews. *Political Science and Politics*, 35(4), pp. 673-676. https://www.jstor.org/stable/1554807

Backman, S. (2023). Risk vs. Threat-Based Cybersecurity: The Case of the EU, *European Security*, 32(1), pp. 85-103. https://doi.org/10.1080/09662839.2022.2069464

Besluit beveiliging network-en Informatiesystemen (Bbni) (2023), Ministry of Economic Affairs and Climate Policy (2023). Den Haag: Nederland.

Boeije, H. (2010). *Analysis in Qualitative Research*. London: Sage Publications Ltd.

Bromiley, P.; McShane, M.; Nair, A & Rustambekov, E. (2014). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning*, 48, pp. 265-276. http://dx.doi.org/10.1016/j.lrp.2014.07.005

Calcara, A. & Marchetti, E. (2022). State-industry Relations and Cybersecurity Governance in Europe. *Review of International Political Economy*, 29(4), pp. 1237-1262. https://doi.org/10.1080/09692290.2021.1913438

Carrapico, H. & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies* 55(6), pp. 1254-1272. https://doi.org/10.1111/jcms.12575

Chiti, E. (2018). Enforcement of and Compliance with Structural Principles. In M. Cremona (Ed.), *Structural Principles in EU External Relations Law* (pp.47-68), Oxford: Hart Publishing. http://dx.doi.org/10.5040/9781782259985.ch-003

CSAN (2022). *Cyber Security Assessment Netherlands 2022*, National Coordinator for Counterterrorism and Security, Ministry of Justice and Security, Den Haag: Nederland, pp. 1-42. https://english.nctv.nl/documents/publications/2022/07/04/cyber-security-assessment-netherlands-2022 [source translated from Dutch, using software Deepl Translator]

CSR (2022). *Meerjarenstrategie 2022-2025*, Cyber Security Raad, pp. 1-29. [source translated from Dutch, using software Deepl Translator]

Cavelty, M.D.& Smeets, M. (2023). Regulatory Cybersecurity Governance in the Making: The Formulation of ENISA and its Struggle for Epistemic Authority, Center for Security Studies, *Journal of European Public Policy*, 30(7), pp., 1330-1352. https://doi.org/10.1080/13501763.2023.2173274

Dinkova, M.; El-Dardiny, R. & Overvest, B. (2020). Cyber Incidents, Security Measures and Financial Returns: Empirical Evidence from Dutch Firms. *CPB Netherlands Bureau for Economic Policy Analysis*, pp. 1-36. https://www.cpb.nl/sites/default/files/omnidownload/CPB-Discussion-Paper-411-Cyber-incidents-security-measures-and-financial-returns.pdf

Directive 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 [2016]. *Official Journal of the European Union* L 194/1, 19 July 2016.

Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union amending Regulation (EU) No 910/2014 and Directive 2018/1972, and repealing Directive 2016/1448 (NIS 2 Directive) [2022]. *Official Journal of the European Union* L 333/80, 27 December 2022.

ENISA (2018). *Guidelines on Assessing DSP and OES Compliance to the NISD Security Requirements. Information Security Audit and Self-Assessment/Management Frameworks*. Athens: Greece. November 2018, pp. 1-59.

ENISA (2022). *ENISA Threat Landscape 2022 (July 2021 to July 2022).* Athens: Greece. October 2022, pp. 1-150. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Enns-Bray, W. & Rochat, K. (2020). Medical Device Regulation and Cybersecurity: Achieving 'Secure by Design' for Regulatory Compliance. *International Journal of Information Secirty and Cybercrime*, 9(2), pp. 12-16. https://www.ijisc.com/year-2020-issue-2-article-2/

European Parliament (2022). *The NIS2 Directive: A High Common Level of Cybersecurity in the EU*, Briefing, EU Legislation in Progress. Brussels: European Parliament, pp. 1-13. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

Groenendaal, J. (2020). Cyber Crises Require Anticipation and Improvisation, *The Hague University of Applied Sciences,* November 2020, pp. 1-5. https://www.thuas.com/sites/hhs/files/images/cyber-crises-require-anticipation-and-improvisation.pdf

Hubbard, D. & Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. In *Why Cybersecurity Needs Better Measurements for Risk* (pp. 55-80). John Wiley & Sons, Incorporated. https://ebookcentral.proquest.com/lib/ucd/detail.action?docID=4585272#

IBRA (2022). *ILT-brede risicoanalyse*. Den Haag: Nederland. September 2022, pp.1-30. https://open.overheid.nl/documenten/ronl-089dab6295bce05136fb221f8350d766dcdf87ac/pdf [source translated from Dutch, using software Deepl Translator]

IJenV (2022). *Cohesive Inspection Picture Cybersecurity Vital Processes 2021-2022*. Den Haag: Nederland, pp. 1-32. https://open.overheid.nl/repository/ronl-a14329a64dca6b92b45a4b2064b9cd13c3524b47/1/pdf/tk-bijlage-samenhangend-inspectiebeeld-cybersecurity-vitale-processen-21-22.pdf [source translated from Dutch, using software Deepl Translator]

Lavenex, S. & Krizic, I. (2022). Governance, Effectiveness and Legitimacy in Differentiated Integration: An Analytical Framework. The International Spectator: Italian *Journal of International Affairs*, 57(1), pp. 35-53. https://doi.org/10.1080/03932729.2022.2035529

Lee, I. (2021). Cybersecurity: Risk Management Framework and Investment Cost Analysis. Business Horizons, *ELSEVIER* 64, pp. 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

Leech, B.L. (2002). Techniques for Semistructured Interviews. *Political Science and Politics*, 35(4), pp. 665-668. https://www.jstor.org/stable/1554805

Leukfeldt, R. (2017). Research Agenda the Human Factor in Cybercrime and Cybersecurity. The Hague: Eleven International Publishing.

Manheim, J.B., Rich, R.C., Willnat, L., Brians, C.L., & Babb, J. (2012). Empirical Political Analysis: An Introduction to Research Methods. Longman Publishing Group.

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 35, *ELSEVIER*, pp. 1-11. https://doi.org/10.1016/j.clsr.2019.06.007

Mastenbroek, E. (2009). *Procedural Legitimacy and EU Compliance, PhD Politics of Compliance* (Doctoral thesis), pp. 1-38. https://repository.ubn.ru.nl/handle/2066/78482

Masters of Digital (2023). *Panel European Cyeber Governance: Bolstering Cyber Security Cooperatinon Across the Union*, 8th of April. In Brussels (online). https://mastersofdigital.org/agenda/

Meuris, J. (2023). 'Port of Antwerp-Bruges', *Railways and waterways: Situation and challenges.* In: Second NISDUC Conference. Brussels: Belgium.

Moneva, A. & Leukfeldt, R. (2023). Insider Threats Among Dutch SMEs: Nature and Extent of Incidents, and Cyber Security Measures. *Journal of Criminology*, pp. 1-25. https://osf.io/eqpb2

Mosley, L. (2013) (eds.). "Just Talk to People"? Interviews in Contemporary Political Science. In *Interview Research in Political Science*. Cornell University Press: Ithaca and London, pp. 1-28. https://edisciplinas.usp.br/pluginfile.php/6653549/mod_resource/content/1/Mosley%2C%20Interview%20Research%20in%20Political%20Science.pdf

National Coordinator for Counterterrorism and Security (NCTV), Dutch Government (2018). *Resilient Critical Infrastructure.* https://english.nctv.nl/documents/publications/2018/02/01/factsheet-critical-infrastructure

National Coordinator for Counterterrorism and Security (NCTV), Dutch Government (2022). *Netherlands Cybersecurity Strategy 2022-2028: Ambitions and actions for a digitally secure society*. Den Haag: Nederland.

National Cyber Sescurity Centre (NCSC), Dutch Government (2018). *National Cyber Security Agenda: A Cyber Secure Netherlands*. Den Haag: Nederland.

National Cyber Security Centre (NCSC), Dutch Government (2020). *Factsheet Risk Management: The Value of Information as Point of Departure.* Den Haag: Nederland. https://english.ncsc.nl/publications/factsheets/2020/september/15/factsheet-risk-management-the-value-of-information-as-point-of-departure

National Cyber Security Centre (NCSC), Dutch Government (2021). *Guide to Cyber Security Measures: Step-by-step to a Digitally Secure Organisation.* Den Haag, Nederland. https://english.ncsc.nl/publications/publications/2021/august/4/guide-to-cyber-security-measures

National Cyber Security Centre (NCSC), Dutch Government (2023a). *Aanpassing in de planning van de nationale implementatie van de Europese CER -en NIS2- richtlijnen.* Den Haag Nederland. https://www.ncsc.nl/actueel/nieuws/2023/juni/16/aanpassing-in-de-planning-van-de-nationale-implementatie-van-de-europese-cer--en-nis2-richtlijnen [source translated from Dutch, using software Deepl Translator]

National Cyber Security Centre (NCSC), Dutch Government (2023b). *Tijdlijn: van EU-richtlijn naar nationale wetgeving.* https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/tijdlijn-van-eu-richtlijn-naar-nationale-wetgeving [source translated from Dutch, using software Deepl Translator]

National Cyber Security Centre (NCSC), Dutch Government (2023c). *Wat gaat de NIS2 richtlijn betekenen voor uw organisatie?* https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie [source translated from Dutch, using software Deepl Translator]

Ogut, H.; Raghunathan, S. & Menon, N. (2011). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, 31(3), pp. 497-512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

Proposal for a Regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices, and agencies of the Union. General approach. Council of the European Union, 2022/0085 (COD), Brussels, 31 October 2022. https://data.consilium.europa.eu/doc/document/ST-14128-2022-INIT/en/pdf

Refsdal, A., Solhaug, B. & Stolen, K. (2015). *Cyber-Risk Management*. London: Springer.

Repko, A.F. & Szostak, R. (2021). *Interdisciplinary Research: Process and Theory* (4edn). Canada: Sage Publications Inc.

RVO (2022). *Standards for Products and Services*. *Government information for entrepreneurs*. https://business.gov.nl/regulation/standards/

Saldaña, J. (2013). *The Coding Manual for Qualitative Researchers* (4edn). United States: Sage Publications Inc.

Second NISDUC Conference From NIS to NIS 2.0 a path to take, 24th and 25th of May, in Brussels. https://www.nisduc.eu/second-conference

- Second NISDUC Conference (2023a). *From NIS 1.0 to NIS 2.0.* Svletana Schuster, Directorate General for Communication Networks, Content and Technology at European Commission.
- Second NISDUC Conference (2023b). *Organising supervision in NIS 2.0.* Panel: Machteld Vrieze, Nicolas Lempereur, Johan Klykens, Tim Mangold and Levi Nietvelt.

Secura (2022). The NIS2 Directive: Perspectives from a Regulator – The Dutch Authority for Digital Infrastructure. In: Secura BV Online 2023 (YouTube). January 24, 2023.

Snyder, H. (2019). Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research*, 104, pp. 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Strupczewski, G. (2021). Defining Cyber Risk, *Safety Science*, 135, pp. 1-10. https://doi-org.ucd.idm.oclc.org/10.1016/j.ssci.2020.105143

The Hackers News (2023, May 2). *Why Telecoms Struggle with SaaS Security*. https://thehackernews.com/2023/05/why-telecoms-struggle-with-saas-security.html

Tigre (2021a). *Assessing Social and Political Trust: A Systematic Review* [Policy Brief], March 2021, pp. 1-6. https://www.tigre-project.eu/resources/TiGRE_PolicyBrief_1.2.pdf

Tigre (2021b). *Trust in Regulatory Agencies: Experts and Citizens Perspectives* [Policy Brief], December 2021, pp. 1-5. https://www.tigre-project.eu/resources/TiGRE_PolicyBrief_2.5.pdf

Timmers, P. (2018). The European Union's Cybersecurity Industrial Policy, *Journal of Cyber Policy*, 3(3), pp. 363-384. https://doi.org/10.1080/23738871.2018.1562560

Weber, F. (2023, May). Compliance is not security! [Text] [Post]. LinkedIn. Retrieved May 2023. https://www.linkedin.com/feed/update/urn:li:activity:7065997156943286272?updateEntityUrn=urn%3Ali%3Afs_feedUpdate%3A%28V2%2Curn%3Ali%3Aactivity%3A7065997156943286272%29

Weiss, M. & Jankauskas, V. (2018). Securing Cyberspace: How States Design Governance Arrangements, *Governance* 32(2), pp. 259-275. https://doi.org/10.1111/gove.12368

Wet Beveiliging Netwer-en Informatiesystemen (Wbni) *voor Digitale dienstverleners,* Ministry of Economic Affairs and Climate Policy (2018). Den Haag, Nederland: Ministry of Economic Affairs and Climate Policy. Accessed: Overheid.nl

Windholz, E. (2012). The Multiple Domains of Harmonisation: Politics, Policy, Process and Program. Australian Journal of Public Administration, 71(3), pp. 325-342. https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1467-8500.2012.00782.x

Wohlin, C. (2014). Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering, *Blekinge Institute of Technology*, 38, pp. 1-10. http://dx.doi.org/10.1145/2601248.2601268

Yasar, K. (2022). Information Security Management System (ISMS), *WhatIs.com,* September 2022. https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS#:~:text=An%20information%20security%20management%20system,impact%20of%20a%20security%20breach.

Yin, R.K. (2009). *Case Study Research: Design and Methods* (4edn). United States: Sage Publications Inc.

Appendix

Appendix A. Dutch critical infrastructure

The Dutch critical infrastructure compiles all the systems, networks, and assets considered essential for the functioning and continuity of Dutch economy's operations ensuring therefore a certain level of security and safety of all the sectors of the country. Among the critical infrastructure, transportation, wires, and Internet cables as well as governmental administration's comprised data are essential in the Netherlands today. But the critical infrastructure follows a similar approach in almost every country with some differences depending on what the focus is on, security-wise.

According to the Dutch Safety Board and Cyber Security Council reports, the Dutch infrastructure could be exploited, or it could be affected by possible counteractions, such as the disconnection of digital infrastructure by countries hit by a digital hack (CSAN, 2022, p. 23). More specifically, within the Dutch critical infrastructure the sectors of energy, ICT, drinking water, water, transport, chemistry, nuclear, financial, public order and safery, digital government and defence are part of the Dutch critical infrastructure. According to NCTV (2018), among the critical processes within those sectors are: i) national transport and distribution of electricity, ii) regional distribution of electricity, iii) Internet and data services, iv) Internet access and data traffic, v) geolocation and time information by GPS, vi) air traffic control, vii) vessel traffic service, or viii) personal and organisational record databases, to name a few.

Appendix B. Sectors of high criticality

Sectors of high criticality as in Annex 1 (NIS2 Directive)

SECTOR	SUB-SECTOR
Energy	(a) Electricity; (b) District heating and cooling; (c) Oil; (d) Gas; (e) Hydrogen.
Transport	(a)Air; (b) Rail; (c) Water; (d) Road.
Banking	
Financial market and infrastructures	

Health	
Drinking water	
Waste water	
Digital infrastructure	
ICT services management (business-to-business)	
Public administration	
Space	

According to the NIS2 Directive different sectors are understood as sectors of high crticiality in the Annex 1 of the Directive. In the Netherlands, the assessment of the level of criticality is performed on the basis of established impact criteria, such as economic damage, physical consequences, or societal developments, such as altered threats or risks, and incident evaluations (NCTV, 2018). Each ministry is responsible for performing the assessment of the critical processes that fall under its responsibility, e.g., safeguarding and inspecting capabilities related to critical infrastructure. In this process, there are numerous stakeholders involved such as governmental institutions, public-private companies, and other types of national and international organisations. Therefore, there is a need for coordination and management of the whole process and that falls under the responsibility of the National Coordinator for Security and Counterterrorism of the Ministry of Justice and Security, which overall manages and ensures cohesion of resilience and increasing measures within the parties involved in the process.

Among the sectors of interest for this research are: digital, transport and public administration sectors. The Human Environment and Transport Inspectorate (ILT) is the supervisor of the Ministry of Infrastructure and Water Management and works on safety, trust, and sustainability in transport, infrastructure, and housing (IBRA, 2022, p.11). The main sectors under the supervision of this inspectorate are high-risk companies; high-risk materials and products; water, soil, and construction; rail and road traffic; shipping; and, aviation.[10] Secondly, the digital infrastructure in society is becoming a target of cyber-attacks, which can lead to social disruption (IJenV, 2022, p. 10). This sector of high

[10] *ILT, sphere of action*. https://english.ilent.nl/about-the-ilt/sphere-of-action

criticality is supervised by the Dutch Authority for Digital Infrastructure (RDI) and under its scope is the energy sector, electricity, gas, oil, and digital infrastructures such as Internet exchanges, DNS, TIOLDs, to name a few. Lastly, the public administration sector is a new sector to be covered by the NIS2 Directive. However, the specific supervisor of this sector and the practicalities for the Netherlands are still to be considered once the Directive is transposed into national law. So far, there are no specifics in the literature or reports about this specific sector. However, this research has gathered information from different public administration entities that can serve as the first steps in this topic.

In the Netherlands, the national legislation that these entities are using is the Wbni and under this legislation, critical service providers are obliged to immediately report all incidents that have significant consequences for the continuity of the service and/or exceed a specific threshold value to the supervisor and the NCSC, the latter has a 24 hours and seven days a week incident response team. Also, ENISA at the EU level (IJenV, 2022, p. 10).

In this regard, the measures implemented in the different sectors differ. For which, the ENISA Threat Landscape 2022 provides insights in terms of trends and patterns across the EU Member States. ENISA is working in parallel on developing sectorial threat landscapes, diving deeper into the elements of each sector and providing targeted insight (ENISA, 2022, p. 7). The report observed that a large number of incidents were targeting public administration, government and digital service providers in the EU (ENISA, 2022, p. 14). This is also relevant because that is the reasoning behind focusing this research on these specific sectors. For instance, in the telecom industry the combination of interconnected networks, customer data, and sensitive information allows cybercriminals to inflict maximum damage through minimal effort (The Hacker News, 2023). The breaches in these type of companies have impactful and far-reaching implications, e.g., reputational damage or sensitive data being stored.

Finally, this report exposes different recommendations for each of the threats analysed during the reporting period. By and large, the recommendations are based in both ISO/IEC 270001:2013 as well as NIST Cybersecurity Framework (CSF). Therefore, in practice, standards such as ISO and NIST are the ones taken into consideration, even

though some speakers in the Second NISDUC Conference (2023) stipulated that others were needed and that was not enough. However, it seems as if in practice these are the rules taken into consideration and even when conducting the interviews some respondents agreed that ISO standards allow for a least burdensome approach in auditing when dealing with less mature organisations, meaning those organisations that do not have the resources, the capacity or the knowledge on cybersecurity risk-management, but that are under the scope of the NIS2 Directive, can take into account the aforementioned standards. The main point taken was that being driven by these standards is easier for medium-sized organisations and larger organisations, because those standards are rather easily understandable and allow to follow best practices in the industry; while at the same time are understood internationally for which cases of industries that operate in different countries might be easier. [11] However, other experts that were speakers at the Second NISDUC Conference argued that 'complying with those standards is not enough and that other actions need to be taken', for which supervisory activities by the competent authorities are needed and duty of care and duty of report of these entities to CSIRTs, single points of contact and, to a lesser extent, supervisory authorities is relevant in the whole process. Because 100% of security does not exist. All in all, it seems widely accepted that these international standards are a first step in cybersecurity risk-management for the critical infrastructure of countries such as the Netherlands.

Appendix C. Ongoing debate

It has been argued extensively that compliance is not anymore the target when dealing with cybersecurity risk-management, but compliance is one part of the process to be resilient in cyberspace, meaning that complying with certain standards and rules (such as ISO 27001 or NIST) does not mean that the public-private institutions as well as governmental institutions or companies more broadly, are secured for future threats and risks in cyberspace. For instance, in one of the panels of the Second NISDUC Conference, one of the speakers said that 'being certified does not equal being secure and following a certain standard does not equal a strategy' (Meuris, 2023). Moreover, it was discussed in

[11] A point made both in the interviews and conferences attended is that a centralisation of policies and procedures facilitates the work of multinationals, telecoms and other organisations with a rather internationalised scope, even though the headquarters are in the Netherlands.

another of the panels of this conference that ‘certification would not resolve the risk completely, it is a way with which you can lower the inspection rate’, while another speaker said ‘we cannot replace inspection because of certification in the Netherlands, certification serves as an information, but being certified it does not equal being compliant’ (Second NISDUC Conference, 2023b). Therefore, the focus now from within the institutions aforementioned is on a more proactive approach, meaning that the standards are there to use, but inspections need to be fulfilled, as well as information-sharing schemes and public-private partnerships with the ultimate goal to reduce the number of risks. This debate is still ongoing since it seems that politicians, business owners, and lawyers do not reach a common ground in this regard. However, the dialogue stage seems an option that all are interested in taking.

Appendix D. Interviews

Interview subjects	Day of the interview
Respondent 1	30th of March; follow-up interview 13th April; 2 hours
Respondent 2	11th of April; 1 hour
Respondent 3	24th of April; two getting-to-know meetings; 1 hour
Respondent 4 (Patrick van de Heisteeg)	28th of April; 1 hour
Respondent 5	10th of May: 50 minutes
Respondent 6	10th of May; one getting-to-know meeting; 1 hour
Respondent 7 (Gijs Peeters)	12th of May; 50 minutes
Respondent 8	22nd of May; 50 minutes

Appendix E. Confidentiality Agreement

Consent form to participate in the study:
"The Dutch Critical Infrastructure: A Cybersecurity Risk-management Approach"

For your participation in the scientific study, we request your consent.

- The researcher(s) provided me with the information of the study and discussed it with me (e.g., the study, my rights/risks, confidentiality, capture/processing/storage/retention period of the interview, and contact information).
- I volunteer to participate in the study. I am fine with being interviewed and know that I do not have to answer everything.
- I am fine with audio recording.
  Yes ☐ No ☐
- I am fine with notes being taken.

  Yes ☐ No ☐
- The researcher(s) will work out the interview on a secure computer that is not connect to the internet and will make my data irreducible as soon as possible after the interview.
- If I want to see my irreducibly transcribed interview, I will contact the principal investigator at the e-mail address below.
- I know that I always have the right to withdraw my consent. After withdrawing my consent, my personal data will not be further processed.
- I understand that the researchers are bound by confidentiality. I will not give names during the interview, for example when discussing cases/examples.
- My unrecognised data may be used by the research team.
- I consent to participate in the research:
  1. Anonimously ☐
  2. Semi-anonimously (only my function is explicitly mentioned by the researcher) ☐
  3. With full credentials (name and function are mentioned by the researcher) ☐

- The researchers comply with laws on data and privacy protection and the Dutch Code of Conduct on Scientific Integrity (VSNU). Therefore, your unrecognised data must be kept fors ome time (maximum 10 years). This rule serves to comply with reliable research.
- If I have any questions later, I know I can contact the principle investigator at: v.gonzalezpouso@hhs.nl

By signing this document, I indicate that I have read the consent form and agree to its contents.

Appendix F. Semi-structured interview questions

These are the main questions shared or asked. However, in some cases during the getting-to-know meeting or the 15 minutes in which I was presenting myself, almost all respondents said that they could not answer these questions, therefore the open questions needed to be asked to be able to continue with the interviews. The questions asked tried to cover as much of the information needed as possible.

1. **Descriptive questions**
    a. **Ground tour question**: Could you walk me through what your organisation did most recently with respect to the issue of cybersecurity/cyber-risks?

    b. **Essential questions for the research**
    - What is according to your organisation cybersecurity risk-management?
    - What are according to your organisation the cybersecurity risk-management measures?
    - Are you aware of a specific EU or national legal framework that mandates these measures?
2. **Core questions**
    a. **Compliance questions**
    - How does your organisation execute these measures and how does it comply with the legal framework you previously identified?
    - Can you give me an example of a situation in which you used cybersecurity risk-management measures?
    - Is there any other type of measures your organisation uses?
    - How do you intend to implement the risk-driven approach to the current/new legal framework mandates?
        - And how do supervisory bodies handle this?
    - **Follow-up question** > Does your organisation have detection systems? If so, what do they entail?
        - What should be reported?

3. **Assessment questions**
    - If there is a change you could make about the approach of your organisation to cybersecurity what would that be?
    - To what extent is there a decrease of the administration bureaucracy between the NIS and the NIS2 Directive?
    - To what extent are you worried you might be liable under the new legislative framework?
    - To what extent do you cooperate with your colleagues working within other sectors of high criticality?
    - To what extent do you coordinate your approaches to cybersecurity with other competent authorities in other critical sectors of the Dutch economy?
    - To what extent do you uniformly implement the Directive's cybersecurity risk-management measures?

- To what extent do you coordinate your approaches with the private sector?
- To what extent do you make use of the double reporting scheme when dealing with incidents?

4. **Other questions asked** (follow-up-questions). Because of the flow of the conversation.

   - How and to what extent does your organisation conduct on-site inspections and off-site supervision, including the identification of weaknesses in databases, hardware, firewalls, encryption, and networks? To what extent does your organisation carry out security audits?

   - How do you perceive the shift from a culture of compliance to a more risk-driven approach, e.g., if a company shows a risk-management culture (e.g., more proactive) is that classified as complying with effectiveness according to your organisation?

   - The NIS2 Directive asks companies of essential and important sectors to implement specific measures to have secure ICT systems. How are you going to monitor these measures in practice? For example, if a company of the sector you are working in has ISO 27000 certifications, are you monitoring their activities or does that imply their cybersecurity measures are complying with your organisation's expectations?

   - What should according to your organisation be reported?

   - To what extent do you use information sharing schemes knowing that trust is key for your organisation? How do you select what information to share and with whom? Is there a policy process for this? Could you walk me through the process?

Appendix G. Coding tree

Due to the length of the coding tree, pictures of it cannot be provided in here. Therefore, the following links are provided to be able to access it. The software used has been Miro:

- https://miro.com/welcomeonboard/d3FYekhGcjBHdmdiemtDM2ZhQ3hJY2taNGlqWG1MdFBvUDBKYjFPYVNTUHJPWjMxYk00QjRLb29Wb0Y3alJqSHwzNDU4NzY0NTE2MzQ0MTQ2ODA1fDI=?share_link_id=408880592013

- https://miro.com/app/board/uXjVMBc0rUg=/?share_link_id=739236779823

Appendix H. Main challenges of NIS Directive

(Second NISDUC Conference, 2023a)

Not all sectors that may be considered critical are in scope.
Diverging incident notification requirements.
Great inconsistencies due to the NIS scope being de facto defined by the Member States (case-by-case basis on OES identification).
Ineffective supervision and limited enforcement.
Diverging security requirements across Member States.
Voluntary and ad-hoc cooperation and information sharing between Member States and between operators.

a. Three main pillars of the proposal for NIS2 Directive

Member State's capabilities	Risk-management and reporting	Cooperation and information exchange
National strategies	Accountability for top management for non-compliance	Cooperation Group
National authorities and SPOCs	Entities are required to take cybersecurity risk-management measures	CSIRTs network
CSIRTs	Entities are required to notify significant incidents	CyCLONe
CVD frameworks		CVD and European vulnerability database
Crisis management frameworks		Peer-reviews