Legislation within cybersecurity: preparing for NIS2 – a detailed framework in the healthcare sector in the Netherlands

Cybersecurity/Turku School of Economics (TSE) & Tilburg School of Economics and Management (TiSEM)

Master's thesis

Author:

Alwin van Welie

ANR: 458030 | SNR: 2099321

Avwelie2000@outlook.com

Thesis supervisors:

First reader: Prof. Dr. A.F. (Anne-Francoise) Rutkowski (Tilburg University)

Second reader: Prof. Dr. H. (Hannu) Salmela (Turku University)

Iris Gulinck MSc (BDO)

Company:

BDO Netherlands

Van Deventerlaan 101

Utrecht, 3528 AG, Netherlands

30.07.2024

Utrecht, the Netherlands

~~Bachelor's thesis~~ / **Master's thesis** / ~~Licentiate thesis~~ / ~~Doctoral thesis~~

Subject: Cybersecurity legislation (NIS2) compliance in the healthcare sector based on a gap analysis and maturity levels for which controls have been derived from known frameworks
Author(s): Alwin van Welie
Title: Legislation within cybersecurity: preparing for NIS2 – a detailed framework in the healthcare sector in the Netherlands
Supervisor(s): Prof. Dr. Anne-Francoise Rutkowski & Prof. Dr. Hannu Salmela
Number of pages: 76 pages + appendices 62 pages
Date: 30.07.2024

Cybersecurity is becoming increasingly important for organizations, particularly in the healthcare sector. In 2023, the healthcare sector was the third most attacked sector of all sectors. Preventing and preparing for cybersecurity incidents is critical in the current digital landscape. The NIS2 Directive is the EU's answer to a more cyber resilient Europe. Preparing to become compliant is not only difficult since the directive has not officially been published yet, but also because compliance is mandatory with the set deadline of the 17th of October, 2024. Non-compliance means big fines which can reach heights as big as 2% of the annual revenue of organizations, or €10 million alternatively. Preventing and preparing for cybersecurity risks is key for the continuation of daily operations. Healthcare organizations do not know how to properly prepare for the NIS2 Directive, nor is there a detailed framework or overview available which specifically addresses the gaps between currently taken measures and yet to be taken measures. This asks for an in-depth gap review of the currently available information regarding the NIS2 Directive to come up with specific controls to prepare for compliance for the healthcare sector, which is what this thesis aimed to do.

By using the Design Science approach, a framework for the Dutch healthcare sector was developed. The framework is created based on a gap analysis. Six gaps were found: incident management, standardized reporting, contact with the CSIRT, standardized impact assessment, mandatory cybersecurity education for management and supply chain cybersecurity assessment. The framework is created based on three iterations, where IT audit, cybersecurity and healthcare experts were interviewed. A NIS2 research involving a thorough understanding of the NIS2 Directive was done to understand the NIS2 Directive's context. A literature review and analysis of frameworks which are often used in IT auditing was then conducted. These frameworks provide the baseline for the created controls for the gaps which were found in a gap analysis between the Dutch healthcare cybersecurity standard NEN 7510 and the NIS2 Directive. The developed framework is verified by ten expert interviews and later validated with two interviews. Required controls in the framework are based on maturity levels to reflect the current level of cybersecurity measures combined with different risk levels within different healthcare organizations.

Key words: NIS2 Directive, cybersecurity, maturity, controls, framework, healthcare, Cyberbeveiligingswet (Cbw), legislation.

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1 Introduction

Cybersecurity is becoming crucial to maintain daily operations within organizations. The world is becoming more digitalized as well, but this comes at a cost. New technologies offer cybercriminals options to exploit flaws in systems or even humans. Countries within the European Union (EU) all deal with this differently, but this severely decreases the collaboration among international, EU-based organizations. As Jalali et al stated in 2019: "*Perhaps there was a time a decade ago when cybersecurity was only a matter of "if" an organization was going to be compromised, but today it has become a question of "when," and "at what level*" (Jalali et al., 2019, p. 66). This asks for a comprehensive cybersecurity legislation which is universal among the EU. The NIS2 directive is the EU's answer to this. NIS stands for Network and Information Security. NIS2 is the successor of NIS1, which is translated into the Dutch law named the Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). The Wbni is also known as the cybersecurity act and focuses on maintaining the confidentiality, integrity, availability and authenticity of network- and information systems. The Wbni states that the organizations in scope have to register incidents as well as taking mandatory measures to prevent or deal better with cybersecurity incidents (Rijksinspectie Digitale Infrastructuur, n.d.).

1.1 Background

Cybersecurity incidents have become one of the biggest problems for organizations the last few years. According to the ENISA threat landscape report of 2023, the most attacked sectors were public administration (19%), targeted individuals (11%), health (8%) and digital infrastructure (7%) (ENISA, 2023). This shows that attacks are not only focused on big companies in the profit sector, but also often at governmental organizations. A recent attack was the hack on the city of Baltimore, Maryland, where a ransom of 13 bitcoin was demanded to regain access to their locked systems. This was crucial to retain the day-to-day activities within the city (Marett & Nabors, 2021). Another example was on eight housing corporations in the Netherlands, which were hit by a hack via their supplier (Verlaan, 2022). Hospitals often become victims of cybercriminals as well. Three hospitals in Germany had to stop offering first aid to patients in need because of a ransomware attack on Christmas Evening in 2023 (Hugo, 2023). Cybersecurity breaches are very costly for organizations (Ogbanufe et al., 2021). An example of this was the ransomware attack on Maastricht University, where the university ended up paying the ransom of 30 bitcoin to regain access to their systems (NOS, 2020). This amounted to €200.000 at the time, which went to cybercriminals instead of to the education system.

In order to prevent cyber incidents as well as properly dealing with them, the EU came up with the NIS legislation. This legislation was implemented differently in different countries. This resulted in organizations not being on the same level in terms of cybersecurity, despite the same legislation being obligatory. What was essential in one country, was not the case in another (The NIS2 Directive, 2023a). An example of this is presented in the impact assessment report on the implementation of the NIS directive. Only a few operators of essential services (OES) were identified for NIS by France and Spain (20.000 per 100.000) in contrast with Italy (90.000 per 100.000). By having more organizations being identified as 'essential', more cybersecurity measures will be taken in a country. This results in consequences as uneven degrees of cyber resilience which could lead to cybersecurity threats crossing nations' borders more easily (European Commission, 2020).

NIS2 is the follow-up legislation which adds more sectors, stricter compliance rules and big fines for all kinds or organizations. NIS2 is meant to increase the cybersecurity and resilience of essential services in EU-member states (Digitale Overheid, 2024a). This is especially hard for the healthcare sector, since they have to focus on delivering health as their main focus, and not proving that they comply to laws. However, the healthcare sector has become an increasingly bigger target for cybercrime, as stated by the ENISA threat report of 2023 (ENISA, 2023). This not only brings threats to the difference between life and death of patients, which is often the case in hospitals such as on the intensive care, but also to the defense of a country as a whole as seen with the COVID-19 pandemic (Kolouch et al., 2021). This is because a key supplier of a critical infrastructure system could be attacked, which could lead to direct outages of information systems used by healthcare organizations such as hospitals. Kolouch et al. (2021) mention that the biggest cyberattack on the University hospital of Brno (which offers 1889 beds) was hit with decommissioning and unavailability of patient data. The unavailability of patient data was not only critical for secure and quality healthcare, but the cost of outages was also enormous: hundreds of millions of CZK (1 million CZK is roughly 40.300 Euro, 100 million CZK would translate to roughly 4 million Euro). This was also during the COVID-19 pandemic, where the hospitals were incredibly busy and often times full or too full. It is therefore critical that healthcare organizations comply with NIS2, not only for compliance reasons. But this proves to be difficult, with not all details being known yet, such as the challenges and gaps between currently implemented controls and measures.

Certain elements of NIS2 are already known, however. Examples are big fines for organizations if they do not comply. NIS2 states that if an organization is identified as an essential company to society, fines can go as far as 10 million euros or 2% of their global annual revenue. For organizations which have been identified as 'important', fines can

go as far as 7 million euros or 1.4% of their global annual revenue (The NIS2 Directive, 2023b). The new legislation was originally planned to go into effect on the 17th of October, 2024. Therefore, organizations are obliged to have everything sorted out at the latest in Q4 of 2024.

Complying to a new legislation is very challenging. Cordella and Iannacci (2010) showed that adoption of e-government policies was difficult to implement. Because of the deadline approaching very soon and difficulties to adopt the new legislation and to comply, there is no time to waste to start working on complying with NIS2. The Dutch government (also referred to as Digitale Overheid) is the main organization in the Netherlands which informs other organizations about NIS2 and how to prepare. They state that organizations can use the BIO, which is a legislation for governmental instances within the Netherlands (Digitale Overheid, 2024b). But the BIO is suited to mostly governmental institutions. Digitale Overheid states on their main webpage that they themselves do not know the specifics of how to properly prepare for NIS2 (Digitale overheid, 2024a). Since organizations need to comply to prevent fines, but they do not know how, a solution is needed.

1.2 Problem statement

Current literature regarding cybersecurity and legislation in the healthcare sector does not offer a comprehensive guide to properly prepare for new legislations. Neither does the company BDO have a framework how to properly implement NIS2 for the healthcare sector, so they are unable to help their customers to prevent big fines. Current literature does offer frameworks which have proved themselves to work however, such as COBIT. These frameworks offer insights into assessing (cybersecurity) risks, and how to improve current situations. Maturity frameworks such as the maturity assessment model presented in the good practice on information security from De Nederlandsche Bank (DNB) can also help with assessing the level of ‘maturity’ for organizations. A new (general) framework to comply to NIS2 which includes specific controls and measures is therefore crucial. One of the main things (top) managers of organizations needs to take into account is the awareness of how cybersecurity elements are perceived and judged by their employees to ensure compliance. This advocates for education, training and awareness of employees regarding cybersecurity (Cram & D’Arcy, 2023). This element is also part of the NIS2 legislation.

IT auditing is an important part of the creation of such a framework. This is because controls are not always presented by the government when directives such as NIS2 are translated into a nationwide law. For example, technical controls are not always presented by the government. An example of this is the following requirement presented in the NIS2 Directive’s official text: “*Essential and important entities should ensure the security of*

the network and information systems which they use in their activities" (European Parliament, 2022, p. 17). Laws often require certain steps or processes to be implemented, but they often do not state how this needs to be done. This means that in practice administrative-, technical- and physical-, and informal controls are not in place to comply to certain laws. Therefore, formal controls with these elements need to be created in order to comply with the NIS2 Directive. Differences between the types of controls have to be studied for this.

Only frameworks which have proved themselves to be useful from the year 2021 or before (with the exception of the DNB framework) will be considered for the development of a new NIS2-framework in the healthcare sector. All these frameworks can be used to create a proper framework which can be used to assess if a healthcare organization is ready for NIS2 and what steps still need to be taken.

1.2.1 Scientific & social relevance

It is a tremendous challenge for every type of healthcare organization to comply to the NIS2-legislation. It is still not entirely clear what NIS2 completely entails. BDO doesn't have a framework to help its customers to comply. Neither can they properly audit NIS2. Organizations are not able to self-assess their current status. This will have major legal implications, such as huge fines (Uniqkey, 2022). Current literature doesn't offer any insights into complying with NIS2, but it does offer frameworks how to implement or change new things because of legislation. A framework how to comply is not only a significant contribution to academic literature, but also a necessary component for BDO to be able to properly and professionally help their customers as well.

1.2.2 Scope of research

Before a suitable framework can be made, current knowledge and literature needs to be reviewed to assess the most usable parts of current frameworks to implement into a new NIS2-framework. First of all, legal documents of NIS2 published by the EU have to be studied in detail. This is part of the research context chapter. Next to this, top IM-journals will be used (see appendix 2), as well as neighboring fields to the IM-discipline and journals from the field of healthcare and law. Differences among NIS and NIS2 need to be compared to find the biggest differences, within the legislation as well as differences among new sectors being added. This will be done in a literature review. The focus will be on the healthcare sector in the Netherlands. All types of healthcare organizations are in scope of this research. Healthcare organizations must use every euro to invest in (services for) their customers, the residents of a country for example, rather than having to spend it on big fines. BDO will help with the research by allowing to use their internal

network of professionals for the research. Since BDO the Netherlands is involved in the research, the scope of the research is also the healthcare sector in the Netherlands. A Design Science approach will be used within this research, since a new artifact (from now on: framework) will be developed. According to Wieringa (2014), a design problem where a new framework should be developed, uses design science which starts with improving a problem context by (re)designing a framework. This framework should satisfy certain requirements, in order to help stakeholders or end-users to achieve a certain goal.

1.3 Research questions

The main research question (RQ) is organized under a set of 4 sub questions (SQ).

RQ: "*How can the health sector in The Netherlands be assessed to determine whether they are compliant with the NIS2-directive*?"

SQ1: What measures are organizations in the healthcare sector currently taking to prepare for NIS2?

SQ2: What are the differences in the obligations within NIS2 among organizations in the healthcare sector?

SQ3: Which parts of current audit frameworks are useful to develop a NIS2-compliance framework for the healthcare sector?

SQ4: Which risks should be covered by a new NIS2-compliance framework to properly assess the current status (maturity level) of different types of healthcare organizations?

1.4 Research design

Since in-depth, (open-ended) interviews will be used as well as written documents, a qualitative research study fits better than a quantitative one (Patton, 2005). A qualitative study generates rich narrative descriptions, which fits with the development of a new framework.

By using several ways to research the identified problem, several methods are used. Brewer and Hunter (2006) state that by using a 'multi-method approach' the quality of the research increases, which adds more value to the developed framework. Below, a visual overview of the research is presented.

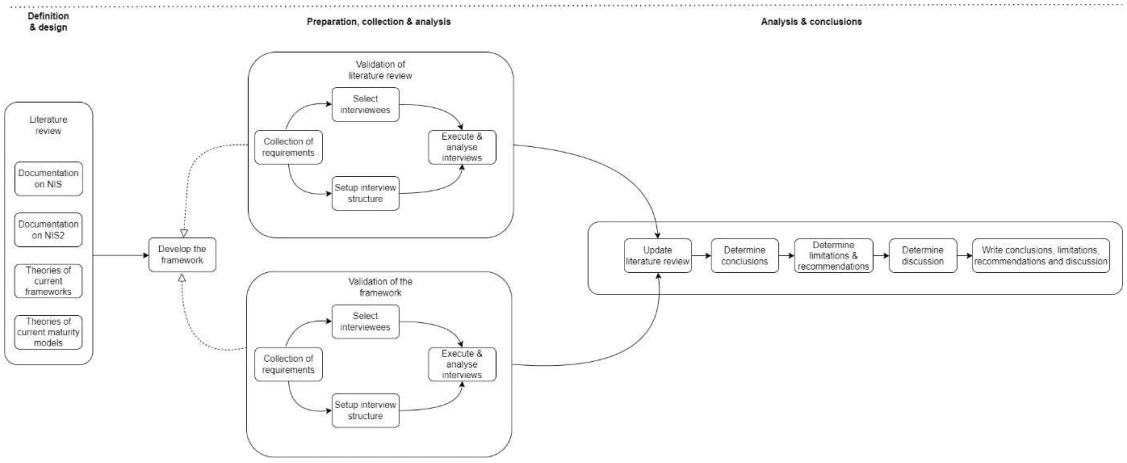


Figure 1: Visual overview of the proposed research

1.5 Structure of the thesis

The thesis is setup so that the NIS2 in context chapter will be done prior to the literature review. When this is done, specific parts of chosen useful frameworks (such as COBIT) will be researched in detail to create the initial NIS2 framework. Next to the literature review, the NIS2 in context chapter will be used for this. The interviews with experts will make sure that the framework is verified and validated. This is explained in paragraphs 4.1.1 and 4.1.2. When this is done, the NIS2 framework will be updated and verified within BDO. This will be done by using documents and use cases of how implementing and starting to comply to a new legislation in the past has been done based on the auditing method ‘cyber in the audit’ which audits cybersecurity implementations in organizations. Senior IT audit experts within BDO with experience in the healthcare sector will be conducted for this. After this is done, the final iterations of the framework will be created. Finally, the conclusions, limitations, recommendations and discussion will be written.

2 NIS2 in context

Before a literature review can be conducted, it is important to have a proper understanding of what NIS2 is, how it works in the Netherlands, and which governmental instances are responsible. Since this information is not available in academic literature, the official documents of both the European Union and the Netherlands will be used to create a NIS2 knowledge base. Other useful sources are also used for the knowledge base. This is a necessary step prior to the actual literature review, since NIS2 is still not finalized in the Netherlands. Finally, it is also important to know how IT auditing works in the Netherlands. This knowledge is useful for the creation of a framework, since preparing for NIS2 also entails being prepared for audits and having relevant controls in place.

2.1 What is NIS2?

NIS2 is based on NIS or NIS1. NIS stands for Network and Information Security. It is a framework presented for all nations among the European Union (EU). NIS1 was originally created to achieve a high common level of cybersecurity across the European Union, with a view to improve the functioning of the internal market (European Union, 2016). NIS2 focuses on not just protecting networks and information systems, but NIS2 also focuses on the broader notion of cybersecurity. This means that the users of attacks coming from cybersecurity threats and other persons affected by these threats are also included in NIS2 in comparison to NIS1. Vandezande (2024) mentions that 160.000 organizations in the entire EU are estimated to fall under NIS2. There will be 10.432 NIS2 organizations in the Netherlands, with 50.000 supply chain organizations linked to these NIS2 organizations (De Snoo, 2024). NIS1 started in the Netherlands with only a few sectors. In the Netherlands, organizations had to comply with NIS1 when they were part of the government, or when they offered digital services (such as online marketplaces, cloud service providers and search engines) (Ministerie van Economische zaken en klimaat, n.d.). NIS2 expanded this scope to other sectors as well. The aim of NIS2 is to achieve a high common level of cybersecurity among all EU nations by improving the functioning of the internal market of the EU (Vandezande, 2024). Since it was a directive from the EU, all member states had to transform the EU's version of NIS to local laws. However, since the directive is open to interpretation for EU's member states, this resulted in major differences in compliance levels (The NIS2 Directive, 2023a). Therefore, the EU figured it was time to increase the scope of organizations which have to comply as well as a more in-depth auditing and the introduction of big fines. With NIS1, big fines could be given to organizations not complying, but this has not happened a lot.

2.2 NIS2: the Dutch case

NIS2 consists of different aspects. First of all, NIS2 shares some common parts with other legislations, such as DORA. Overlapping parts are mentioned in the application of article 4(1) and article 4(2) of the NIS2 Directive[1]. These articles lay the foundation for NIS2's operational framework. Essentially, these two articles are providing a roadmap to ensure a harmonious and effective approach to cybersecurity (Spiteri, 2023). This is important, since organizations don't want to have everything sorted for NIS2, where DORA states on a specific topic that the organization does not comply. Finally, member states have to ensure that any natural person in charge of the entities (or someone who acts as a legal representative on the basis of the power to represent it), can be held liable for breaching their duties to ensure compliance with NIS2 (European Parliament, 2022). Secondly, NIS2 is a directive. This is different from regular legislation. The European Union (EU) distinguishes five types of legislations: regulations, directives, decisions, recommendations and opinions. A directive is a legislative act which all countries in the EU must achieve. It is up to the countries specifically how to reach these goals. The EU set up the baseline of NIS2; nations can choose how to implement these into local laws themselves (European Union, n.d.).

To prepare for NIS2, several organizations or authorities have come up with so-called 'quick scans'[2]. These 'scans' are in practice a set of questions which need to be answered in order to answer the question if an organization is in scope of NIS2. However, the quickscan from the Dutch Government states that the outcomes are not final, and that no rights can be derived from the scan outcome (Rijksoverheid, 2024). This still leaves organizations in the dust with almost no direction to head towards without such specific technical controls. An example: "*Essential and important entities should ensure the security of the network and information systems which they use in their activities*" (European Parliament, 2022, p. 17). In practice, administrative-, technical- physical-, and informal controls are not pre-determined to comply to NIS2. Therefore, formal controls with these elements need to be created in order to comply to certain laws such as the Dutch translation of the NIS2 directive.

Implementation of NIS2 in the Netherlands

In order to prevent cyber incidents as well as properly dealing with them, the EU came up with the NIS legislation. This legislation was implemented differently in different

[1] Article 4(1) and article 4(2) of the NIS2 provides clarification on the application of cybersecurity risk-management incidents reporting and measures requirements (European Commission, 2023b).
[2] An example of a quick scan is available on the official Dutch Governmental website: https://nis2zeker.nl/

countries. This resulted in organizations not being on the same level in terms of cybersecurity. What was considered essential in one country, wasn't in another (The NIS2 Directive, 2023a).

As explained above, each nation within the EU is free to choose how they implement the directive. In The Netherlands, the Wet beveiliging network- en informatiesystemen (Wbni) is the Dutch translation of NIS1. NIS1 entailed an obligation to report incidents, as well as a duty to take measures to set up or improve (cyber) security (Ministerie van Algemene Zaken, 2023). The name of the NIS2 directive translated into a Dutch law will be 'cyberbeveiligingswet' or Cbw in short (which translates to cybersecurity law) (Digital Trust Center, 2024).

The EU noticed that, together with the enormous increase in cyber-attacks as well as organizations simply not complying properly with the law, something had to happen. NIS2 is the follow-up legislation which adds more sectors, stricter compliance rules and big fines for all kinds of organizations. NIS2 is meant to increase the cybersecurity and resilience of essential services in EU-member states (Digitale Overheid, 2024a).

There are minimum measures that organizations need to implement if they are in the scope of NIS2. Based on the size of the business, the societal function and how exposed the organization is, the level of requirements may vary. The Dutch 'Digital Trust Centre' is part of the Ministry of Economic Affairs and Climate. The Digital Trust Centre stated that even though NIS2 lays a foundation with steps to comply which can be expanded, the Dutch government chooses to only translate the parts from the European NIS2 version which are strictly mandatory (Digital Trust Center, 2023). For these minimum measures to be implemented, specific controls need to be created. Since it is not clear what specific controls should be in place, specific controls could be based on IT audit frameworks which already assure compliance with certain minimum measures.

The organization Samen Digitaal Veilig, which is an initiative of MKB-Nederland[3] and VNO-NCW[4] states in a webinar that the current deadline will not be in the autumn of 2024, but rather in the spring of 2025 (De Snoo, 2024). Finally, it is expected that the Cbw will go into effect in the 'second or third quarter of 2025' (Yeşilgöz-Zegerius, et al., 2024).

New in NIS2: Four obligations

In general, NIS2 comes down to four parts. These four parts are 1) obligations to adopt certain (national) cybersecurity strategies, 2) setting up cybersecurity risk management measures as well as reporting duties, 3) new rules and 4) obligations regarding data

[3] MKB-Nederland is an organization which looks after the interests of SMEs in the Netherlands (MKB-Nederland, 2024).
[4] VNO-NCW is an organization which is a business association with branch organizations as members who collaborates with the Dutch government (VNO-NCW, 2024).

sharing of cybersecurity information and supervisory and enforcement obligations of member states (European Parliament, 2022). The following paragraphs discuss each part in more detail.

2.2.1 Part 1 of NIS2: adopting cybersecurity strategies

The first part of NIS2 entails obligations which requires all member states to adopt certain (national) cybersecurity strategies. They will have to establish and set up competent authorities, cyber crisis management authorities, and single points of contact (regarding cybersecurity). Finally, nations will have to set up Computer Security Incident Response Teams (CSIRTs).

A network of CSIRTs has to be established within the nation. The European Commission will participate as an observer in the network, where ENISA will provide the secretariat. ENISA is the European Union Agency for Cybersecurity. ENISA contributes to the EU cyber policy. It does this by enhancing the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, by cooperating with EU bodies and different member states. ENISA is dedicated to achieving a high common level of cybersecurity across all member states within the EU (ENISA, 2024). ENISA will also actively provide assistance for the cooperation among the CSIRT (European Parliament, 2022). CSIRT's tasks can be divided into five general tasks. Which are monitoring, analysis, incident response, directing, and coordination.

Each member state assigns at least one (preferably more) CSIRTs for the nation. Within the Netherlands, the CSIRT tasks for organizations which fall under the ministry of Economic Affairs and Climate are centralized at the National Cyber Security Centre (NCSC) for example. The Netherlands will have several CSIRTs to report to. Depending on the type of sector, there are different CSIRTS to report to (Digital Trust Center, 2023). The Dutch healthcare sector has a specific CSIRT to report to, which is called Z-CERT. This organization is a collaboration (non-profit) between the foundation of the Dutch Association of University Hospitals, GGZ and the Dutch Ministry (Kamara & Van Den Boom, 2022).

2.2.2 Part 2 of NIS2: setting up cybersecurity risk measures & new reporting duties

The second part of NIS2 entails that organizations have to set up cybersecurity risk management measures. Organizations will also have new reporting duties. This is obligatory to organizations which are either regarded as essential or important. The difference between essential and important sectors will be discussed in paragraph 2.2.4.

The European Commission has come up with ten measures which (at least) need to be taken into account for organizations within the NIS2 scope. This is visualized below:

Measure number	Measure
1	Creating or updating policies on (one or more) risk analyses and information system security.
2	Incident handling.
3	Business continuity (management), such as backup management and disaster recovery and crisis management.
4	Security for the supply chain, including security related aspects which concerns the relationship between its direct suppliers or service providers and between each entity.
5	Security in the network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.
6	Policies and procedures have to be in place to assess the effectiveness of (the) cybersecurity risk management measures.
7	Basic cyber hygiene practices and cybersecurity (awareness) training has to be done.
8	Policies and procedures regarding the use of cryptography have to be in place. When necessary, encryption has to be included as well.
9	Human resources security, access control policies and asset management have to be in place.
10	The use of Multi-Factor Authentication (MFA) or continuous authentication solutions have to be implemented. Secured voice, video and text communications have to be prepared and implemented as well as secured emergency communication systems within the entity, if necessary.

Table 1: NIS2's ten new measures (European Parliament, 2022).

One part that needs to be done is risk management. This entails implementing improvement measures to minimize risks as well as potential consequences. Incident management, supply chain security, network security, access control, and encryption needs to be added to organizations' day to day activities (The NIS2 Directive, 2023c). Interestingly, no guidelines are provided in order to improve such organizational management tasks.

The security of the supply chain of information is one of the new obligations with the coming of NIS2. For this reason, organizations will have to look into their current partnerships with both information receiving and information sending organizations. Suppliers of IT solutions may still be hacked which will have an impact on the service they provide to other organizations.

2.2.3 Part 3 of NIS2: new rules and obligations regarding data sharing of cybersecurity information

Part 3 of NIS2 entails that organizations have to deal with new rules and obligations regarding the data sharing of cybersecurity information.

Within 24 hours of an incident (depending on the severity), an incident needs to be reported to the CSIRT or competent authorities. Reporting can be done at the reporting desk, which is open twenty-four seven, every day (Digital Trust Center, 2023). This only has to be done when an incident is considered significant. An incident is regarded as significant when it leads to one of the following:

- An operational disruption within the organization;
- Financial losses within the organization;
- Creating disruptions for other organizations (Digital Trust Center, 2023).

Reporting the incident this early means that an indication of the significance and severity of the impact has to be estimated, since this is not entirely clear at the time. Next to this, an indication of if the incident will have unlawful, malicious or harmful acts must also be reported. Finally, it must be reported if the incident may have an impact cross the borders of the nation the organization is located in (European Parliament, 2022).

Within 72 hours, an incident notification, which (if applicable), has to update the information referred to as reported in the incident report in the first 24 hours after the occurrence. It must indicate an initial assessment of the significance of the incident, including its severity and impact, as well as (if applicable), the indicators of compromise.

After no later than one month after the incident, a submission of the incident as reported in the 72-hours post incident report has to be submitted. It must include a detailed description of the incident, including its severity and impact, the threat type or root cause which was likely to have triggered the incident, the ongoing as well as applied mitigation measures, and finally (if applicable), the cross-border impact of the incident (European Parliament, 2022).

Finally, nations can also choose to voluntarily report an almost-incident. This way, the entire network of connected organizations to NIS2 can learn from each other. By doing this, you could receive help from a CSIRT to help improving the cybersecurity measures taken into a specific organization. This may be very useful, since the extra capacity to work on this is available from CSIRTS where not every organization has the time to work on this. There will be no (potential) negative effects of reporting an almost-incident to the reporting desk (Digital Trust Center, 2023).

2.2.4 Part 4 of NIS2: supervisory and enforcement obligations as a member state of the EU

Part 4 of NIS2 entails new supervisory and enforcement obligations of Member States.

One of the newly added international groups within NIS2, is the EU European Cyber Crisis Liaison Organization Network (CyCLONe). This network is set up to support the coordinated management of large-scale cybersecurity crises and incidents at an operational level. EU CyCLONe will also ensure the regular exchange of relevant

information among (European) Union institutions, bodies, offices, agencies and Member States. EU-CyCLONe has to be composed of the member states' cyber crisis management authorities representatives, as well as the (European) Commission (in the case of large-scale cybersecurity incidents). ENISA will provide the secretariat of EU-CyCLONe, as well as supporting the secure exchange of information. They will also provide necessary tools to support coordinating among and between member states of the EU (European Parliament, 2022).

At least every two years, starting from the 17th of April 2025, each member state must provide a list of all essential and important organizations in their respective country (European Parliament, 2022). When an organization spans more than just one country, all responsible (supervision) authorities have to cooperate, and if needed, carry out joint tasks. Exceptions to this are public administration entities, providers of public electronic communications networks or publicly available electronic communications services, and certain types of entities which are under the jurisdiction of the Member State[5].

NIS2 states that if an organization is identified as an essential company to society, fines can go as far as 10 million euros or 2% of their global annual revenue. For organizations which have been identified as 'important', fines can go as far as 7 million euros or 1.4% of their global annual revenue (The NIS2 Directive, 2023b). The new legislation goes into effect on the 17th of October, 2024. The original publication of NIS2 in the Europe Union was on the 14th of December, 2022 (European Parliament, 2022). Authorized authorities are able to determine a final date for measures to be implemented if the results of an audit are that an infringement of the Cbw has been committed (Overheid.nl, 2024).

All organizations which are essential or important according to NIS2 have to comply with NIS2. NIS2 has divided organizations in one of the two, based on their size and/or annual revenue.

- An organization is considered essential if it has at least 250 employees, or an annual revenue of 50 million or more or a balance total of 43 million or more.
- An organization is considered important if it has 50 employees or more, or an annual revenue of 10 million or more (Digital Trust Center, 2023).

The mandatory requirements are the same for both essential and important organizations. The supervision of how NIS2 is implemented is different. When an organization is considered essential, supervision will be done in a proactive manner. When an organization is considered important, supervision will be done in a reactive manner (Digital Trust Center, 2023).

[5] A list of all entities are presented in Appendix 1.

2.3 Different types of organizations part of NIS2

NIS2 introduces new sectors to the original NIS directive. The difference is between "essential" and "important" organizations. The European Union has created a list of the organizations which are either part of annex 1 or annex 2. Annex 1 describes very critical sectors, and annex 2 describes other important sectors. However, NIS2 establishes a differentiation of supervisory regimes (European Commission, 2023a). This means that there will be different authorities and independent parties responsible for either the 'essential' or the 'important' sectors, as specified by NIS2. The idea is to create a fair balance of obligations between both the responsible authorities and the organizations (European Commission, 2023a).

Every nation has to decide themselves which organization monitors NIS2. Within the Netherlands, a general foundation is found in the different ministries. Every ministry has a certain authority which is suitable and assigned to be responsible for specific sectors. The responsible authorities for the NIS1 in the Netherlands are explained in the document 'samenhangend inspectiebeeld cybersecurity vitale processen' (translated: the report on the inspection of cybersecurity and vital processes) by the Ministry of Economic Affairs and Climate. For the Netherlands, this report presents almost all authorities which are responsible for a specific sector. This document presents the current state of responsible organizations within the NIS1 (Wbni) scope. It is likely that these responsible authorities will stay the same for NIS2, where some other responsible authorities will have to be added. The Dutch translation of the NIS2 Directive, the Cbw, states that the waste sector is part of the ministry of Infrastructuur and Waterstaat which the Inspectie Leefomgeving and Transport (ILT) is responsible for (Overheid.nl, 2024).

All sectors presented in Annex 1 and Annex 2 for the NIS2 Directive have been presented in the report, with the exception of the production, processing and distribution of food sector (Ministerie van Economische Zaken en Klimaat, 2023). However, since in the past is has been shown that the Netherlands Food and Consumer Product Safety Authority (NVWA) has been responsible for food-related legislations for the ministry of health, welfare and sports, the NVWA[6] will most likely be responsible for the production, processing and distribution of food sector. The overview is as follows:

Table 2: Overview of sectors and auditing authorities in the Netherlands

Sector	Annex	Type	Responsible authority	Example

[6] For the production, processing and distributing of food sector, it has not been specified in NIS1 which organization is responsible for the sector. However, in general in the Netherlands, the Nederlandse Voedsel en Waren Autoriteit (NVWA) is in charge of inspecting the quality of food. Therefore, the assumption has been made that this authority will be responsible for organizations that are present in the production, processing and distributing of food sector.

Energy	1	Essential	Rijksinspectie Digitale Infrastructuur (RDI)	Suppliers or distributors of energy such as electricity organizations, heating and cooling organizations, and oil, gas and hydrogen using or creating organizations.
Transport	1	Essential	Inspectie Leefomgeving en Transport (ILT)	Aerial transport (planes, helicopters), railroad organizations (such as trains), road organizations (such as creators of concrete for roads or decision-makers who decide on new roads as well as organizations who transport things through the road), sea transport organizations.
Banking	1	Essential	De Nederlandsche Bank (DNB)	Organizations working with credit, organizations which main profession is to trade (on the stock market for example), as well as market- and infrastructure organizations.
Financial market infrastructures	1	Essential	De Nederlandsche Bank (DNB)	Organizations working with credit, organizations which main profession is to trade (on the stock market for example), as well as market- and infrastructure organizations.
Health	1	Essential	Inspectie Gezondheidszorg en Jeugd (IGJ)	Organizations which research health, productors of health (solutions), health providers (such as hospitals, dentists), and manufacturers of health (solutions), such as vaccination creators for diseases.
Drinking water	1	Essential	Inspectie Leefomgeving en Transport (ILT)	Organizations which are in charge of drinking water as well as distributing waste water, such as Vitens.
Waste water	1	Essential	Inspectie Leefomgeving en Transport (ILT)	Organizations which are in charge of drinking water as well as distributing waste water, such as het Waterschap and local municipalities.
Digital infrastructure	1	Essential	Rijksinspectie Digitale Infrastructuur (RDI)	Organizations that distribute and manage DNS (addresses), trust services organizations, data center services organizations, cloud computing organizations, communication services organizations, managed service providers organizations and managed security providers organizations.
ICT service management (B2B)	1	Essential	Rijksinspectie Digitale Infrastructuur (RDI)	See digital infrastructure
Public administration (governmental services)	1	Essential	Autoriteit Persoonsgegevens (AP)	Municipalities and regions, such as ‘municipality Utrecht’ and the ‘province Utrecht’.
Space	1	Essential	Rijksinspectie Digitale Infrastructuur (RDI)	Software and services organizations which help with space activities are part of this group.
Postal and courier services	2	Important	Rijksinspectie Digitale Infrastructuur (RDI)	Organizations which are in charge of parcel services, such as PostNL and UPS.
Waste management	2	Important	Inspectie Leefomgeving en Transport (ILT)	Organizations such as AVRI which take care of managing waste are part of this group.

Manufacturing, production and distribution of chemicals	2	Important	Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)	Organizations which produce and distribute chemical products.
Production, processing and distribution of food	2	Important	Nederlandse Voedsel en Warenautoriteit*	Organizations which produce food products as well as distributors of foods.
Manufacturing (general)	2	Important	Rijksinspectie Digitale Infrastructuur (RDI)	Organizations which produce medical devices, computers and electronics, machinery and equipment, motor vehicles, trails and semi-trailers and other transport equipment.
Digital providers	2	Important	Rijksinspectie Digitale Infrastructuur (RDI)	Online marketplaces such as Amazon and eBay, search engines such as Google, Bing and DuckDuckGo, and social platforms such as Facebook and LinkedIn.
Research	2	Important	Rijksinspectie Digitale Infrastructuur (RDI)	Organizations (often present within universities) which are responsible for researching current or new topics such as new technologies.

3 Literature review

Based on the research question, keywords will be derived. The research question is as follows: **RQ: "*How can the health sector in The Netherlands be assessed to determine whether they are compliant with the NIS2-directive?"***

The research question consists of several parts. The keywords of the literature are derived from the research question. They are as follows:

- "healthcare", "compliance", and "cybersecurity";
- "Maturity assessment" and "legislation";
- "NIS2".

Next to these keywords, it is important to delve into IT auditing. Since NIS2 is a legislation which means that compliance is important, it will have to be audited. This will be discussed first.

3.1 IT auditing

An audit is an examination of several aspects of an organization. This examination, which is systematic and objective, compares what the organization does to a defined set of criteria or requirements. Often times, an audit is defined as an independent examination, review or inspection. The term applies mostly to financial statements or accounts, but is applied to various examinations of many different subjects within organizations. Information Technology (IT) auditing examines controls, processes and IT assets. It does this at multiple levels within an organization, in order to determine the extent to which an organization adheres to certain requirements or standards (Gantz, 2013)[7].

IT auditing "*helps organizations understand, assess, and improve their use of controls to safeguard IT, measure and correct performance, and achieve objectives and intended outcomes*" (Gantz, 2013, p. 17). IT auditing uses formal auditing methodologies to examine IT-specific capabilities, processes and assets, as well as their role in enabling the business processes of an organization. Next to this, IT auditing also addresses capabilities or IT components which support other domains. Examples of these domains are financial management and accounting, operational performance, quality assurance, governance, risk management and compliance.

[7] Stephen D. Gantz is an information security and IT consultant with over 20 years of experience in privacy management. He currently holds an executive position with a health information technology services firm serving federal and state governments customers. Gantz is also an Associate Professor of Information Assurance. Gantz wrote an often-used book to teach IT auditing (Amazon, 2024). This makes Gantz an excellent source which is therefore used frequently when looking into the IT audit subject.

IT audits can be executed by internal auditors of an organization, as well as by external auditors. The procedures and processes for executing an IT audit are often quite similar in both internal and external auditing. The difference is that the roles of the audited organizations as well as its personnel can be markedly different (Gantz, 2013).

It is important that organizations are prepared for IT audits, since organizations often use them to "*satisfy legal or regulatory requirements, assess the operational effectiveness of business processes, achieve certification against specific standards, demonstrate compliance with policies, rules, or standards, and identify opportunities for improvement in the quality of business processes, products, and services*" (Gantz, 2013, p. 17).

3.1.1 Internal controls

Audits share a common focus. This is the implemented internal controls and how they are maintained. Controls are "*a central element of IT management, defined and referenced through standards, guidance, methodologies, and frameworks addressing business processes; service delivery and management; information systems design; implementation and operation; information security; and IT governance*" (Gantz, 2013, p. 28).

Internal controls are a combination of auditing activities. The maintenance and implementation of a set of controls within an organization is presented to mitigate any possible risks. This is because the controls are the things which are examined, analyzed, evaluated or tested. Organizations often prepare for audits by implementing several internal controls to achieve control objectives (Gantz, 2013).

There are several types of internal controls, which are based on their function. First of all, there is a difference between formal and informal controls. Formal controls refer to the officially sanctioned mechanisms (which are often times codified). These include written rules, procedural directives and standard operating systems. They are objective, visible controls. Informal controls refer to less objective, uncodified controls. The main difference is the level of explicitly and visibility (Kreutzer et al., 2016). Different types of controls include administrative controls, technical controls, and physical controls. Administrative controls include the procedures, policies and plans of organizations which specify what an organization plans to do in order to protect the integrity of its operations and information. Technical controls entail the mechanisms, which include technologies, operational procedures and resources, implemented and maintained in order to reach its control objectives. Finally, physical controls entail the provisions of an organization in order to maintain, restrict, keep available, or monitor access to physical locations. These locations can be storage areas, equipment, facilities and information assets. The most used physical locations are server rooms and datacenters. Next to this, there are three purpose-based categories regarding internal controls. These include preventive, detective,

and corrective controls. Preventive controls entail organizations trying to keep unwanted events from occurring. Detective controls entail the discovering of why unwanted events have happened. Corrective controls help with responding and/or recovering from unintended events (Gantz, 2013).

3.1.2 IT Auditor types

Different kinds of organizations and individuals could conduct several types of audits. Within the Netherlands, NOREA is the professional association which is needed to become a certified IT auditor (NOREA, n.d.). To become certified, a postmaster has to be done. The different types of auditors are:

- Internal auditors or contractors, (hired) outsourced specialists or consultants which execute internal audits;
- IT auditors not working under a contract neither as an employee of a professional service;
- Specialized accounting or auditing organizations (or the audit/accounting departments of these organizations);
- Certification organizations which are authorized to evaluate controls and practices;
- Firms with the authority to oversee implementations of certain controls which are required or enforced because of certain legislations/regulations;
- Inspectors in general, audit executives or any other equivalent officially authorized auditors to execute independent reviews for the organizations for which they work (Gantz, 2013).

Next to this, the audits conducted by authorized instances are also different in nature. The scope of IT audit activities can range on various levels. This is because the wide range of required skills and experience as well as the primary objectives of the type of audit depends significantly on the scope of the to be performed audit. The different levels are as follows:

- Organizational audit (broadest level);
- Internal control audit;
- Information technology audit;
- Information system audit;
- Security control audit (Gantz, 2013).

3.1.3 Often used standards, terms and frameworks within IT auditing

Within IT auditing, certain instances offer specific standards to properly execute an IT audit. This paragraph will look into the most important and known frameworks,

standards, instances and assessments which help by preparing for a future audit or legislation. At the end of the paragraph, an overview of all different standards and frameworks is presented. This overview is used to assess the most important frameworks and standards to be used for the creation of the NIS2 framework.

3.1.3.1 ISO/IEC/NEN

ISO/IEC and NEN are frequently used frameworks within the professional field. For example, the ISO/IEC 27001 standard is one of most commonly used standards regarding information security globally (Malatji, 2023).

One of the most well-known standards is set by the International Organization for Standardization (ISO). ISO offers standards which help with environmental-, quality-, information security-, risk management, & IT governance. ISO offers several standards for different types of organizational needs. IEC stands for International Electrotechnical Commission. IEC offers guidelines, instructions, definitions or rules which are used to design, install, manufacture, certify, test and repair electronical systems and devices (International Electrotechnical Commission, n.d.). NEN stands for Stichting Koninklijk Nederlands Normalisatie Instituut, which translates to the Royal Foundation of Dutch Normalisation Institute. NEN offers norms and guidelines, which are based on connecting parties and stakeholders that discuss these norms and guidelines. NEN also offers support in applying and training these norms in practice (NEN, n.d.-b). NEN is the most important instance which offers norms in the healthcare sector in the Netherlands. NEN implements these norms by looking at original ISO and IEC norms. A few of the most important norms for ISO, IEC and NEN for IT auditing (Malatji, 2023; Broderick, 2006; Gulinck; 2024) are mentioned below.

ISO/IEC 27001: cybersecurity controls in general

ISO/IEC 27001 is a very well-known cybersecurity framework. Both ISO and IEC have jointly developed the 27001 version of ISO. ISO/IEC 27001 offers best-practices and information security controls for managing information security risks. Next to this, it also describes requirements to help maintaining, improving and implementing an Information Security Management System (ISMS) over time. In general, ISO/IEC 27001 helps organizations of any size in any industry protecting their sensitive information in a cost-effective way by defining a framework which can be implemented (Toussaint et al., 2024; ISO/IEC 27001:2022, n.d.).

NEN 7510: cybersecurity in the Dutch healthcare system

One of the most important cybersecurity standards within healthcare is the NEN 7510 standard. This framework is often compared with ISO/IEC 27001. This is because it is

based on ISO/IEC 207001 (NEN, n.d.-a). It provides guidelines as well as basic principles which help with determining, establishing and maintaining measures. An organization in the health care sector can take these to secure the provision of information (NEN, 2020).

NEN 7510 is mandatory for healthcare providers. Despite NEN 7510 being a norm, healthcare instances require the norm to be implemented (it is obligatory) (NEN, n.d.-c). NEN 7510 is also recommended for all organizations which have any connection with the healthcare sector, such as data processors. The Inspectie Gezondheidszorg en Jeugd (IGJ) is responsible for checking if healthcare sector is sufficiently protecting its (patients) data. According to the IGJ, in 2022 only twenty three out of seventy-seven hospitals in the Netherlands complied with the norm of NEN 7510. In 2023, their expectation was that seventy out of seventy-seven hospitals would comply to the norm (Inspectie Gezondheidszorg en Jeugd, 2023).

By complying with NEN 7510, organizations will have some parts already covered in comparison with NIS2. This is because there are overlapping parts between ISO/IEC 27001 and NEN 7510, since parts of NEN 7510 are based on ISO 27001 (NEN, n.d.-a). For example, part two of NIS2, which entails setting up cybersecurity risk measures as well as new ways of having to report incidents, is already covered by NEN 7510 (Ministerie van Volksgezondheid, Welzijn en Sport, 2023).

3.1.3.2 COBIT

Another well-accepted framework is the Control Objectives for Business and Related Information Technologies (COBIT) framework. It is a framework created for information technology (IT) management and IT governance (ISACA, n.d.). The framework is nowadays one of the most commonly used models for both management and IT governance. The primary goal of COBIT is to focus on sufficient governance practices rather than audits or compliance. However, COBIT describes principles, processes and enablers in a detailed, hierarchical way which provides a baseline for executing IT audits. The latest version, COBIT 5, combines key principles from other known frameworks, such as ITIL and several other ISO standards (Gantz, 2013). COBIT presents a CMMI-based process capability scheme to measure maturity (ISACA, 2018).

3.1.3.3 ITIL

ITIL is another well-known framework. It stands for Information Technology Infrastructure Library. ITIL defines the skill requirements and organizational structure of an IT organization. Next to this, it defines a set of standard operational management procedures and practices to manage infrastructures and IT operations (ITIL open guide, n.d.).

ITIL is therefore a governance model which describes a start-to-end life cycle. Next to this, it also provides an integrated set of guidance as well as practices in the areas of service strategy, transition, design and operation, which includes incident management steps.

3.1.3.4 NIST

NIST stands for the National Institute of Standards and Technology. NIST provides security control assessment guidance documents on information security and privacy management (Gantz, 2013). Specifically, NIST offers the cybersecurity framework (CSF). NIST was developed in collaboration between both governments and industries. The framework offers a prioritized, flexible, repeatable and cost-effective approach to managing cybersecurity risks. It does this for applications of critical infrastructure environments. Next to this, it also mentions explicitly that not every organization has the same cybersecurity risk management needs (Toussaint et al., 2024). This means that different levels and levels of cybersecurity investments have to be done within different types of organizations.

3.1.3.5 COSO

COSO stands for the Committee of Sponsoring Organizations of the Treadway Commission. COSO offers a framework which is called Internal Control Integrated Framework. An example of COSO's frameworks is the framework for enterprise risk management (ERM). Their ERM framework helps with setting up a well-functioning organizational- and governance structure. The framework also describes relevant principles, components and concepts of ERM, which are all applicable to every type of organization (Beulen & Ribbers, 2021). This makes the framework generally applicable, which is not the same for NIST but it is for ISO/IEC 27001 for example.

3.1.4 Reporting within IT audit

Within IT auditing, there are several ways in which an IT audit can be presented. Based on if the report should be an advice, just a list of findings or a combination including recommendations, the types of reports are different.

3.1.4.1 Assurance reports

An assurance report demonstrates that third-party service providers' operations and services match the agreements of customers. It also shows that these agreements are matching with (international) standards. The goal of such reports is to gain an overview into how risk management, information security, and processes are dealt with by the third-

party service provider. Examples of this are the ISAE3402, SOC1, SOC2, SOC3 and ISAE3000.

ISAE stands for International Standard on Assurance Engagements. ISAE is an international assurance standard. It describes the Service Organization Control (SOC) engagements. This provides assurance to a customer of an organization that the audited organization has sufficient internal controls in place. ISAE3402 is also known as SOC1. SOC2 is the follow-up version of this, focusing IT services, as of 2016. The original ISAE3402 setup is still used for several types of service organizations (Gulinck, 2024).

Where SOC2 is privately published within the organization, SOC3 can be published openly on the website of an organization (NOREA, 2021). This can have advantages, such as more trust from potential customers. Another example is ISAE3000. This international assurance standard works the same as the ISAE3402, but it is specifically for non-financial statements (International Auditing and Assurance Standards Board, 2013).

3.1.4.2 Report of factual findings

A report of factual findings is a report which is not specifically targeted towards a certain period of time, or on an annual account. The report does not consist of a judgement of an independent auditor. The final judgement has therefore to be made by the audited user or organization themselves (The Audit Generation, n.d.). An example of this type of report is the 4400 report. It shows an organizations' responsibilities when engaged to perform an agreed-to procedures engagement. The 4400 report also deals with the content and form of the agreed-to procedures report (International Auditing and Assurance Standards Board, 2020). For the Netherlands, NOREA owns the right for producing and updating the 4400 report (NOREA, 2022).

3.1.4.3 Advisory reports

Within an advisory report, not only findings are reported. A recommendation of steps to be taken based on the findings is also presented (Gulinck, 2024; AACA, n.d.). There are different types of assurance and consultancy activities. All of these activities may come in another form of internal audit, such as in an advisory report (Chartered institute of Internal Auditors, 2023).

3.1.5 Frameworks within IT auditing

As mentioned before, there are a few important frameworks which are used within IT auditing. An organization which has created a framework to determine where an organization is currently at in terms of cybersecurity, is the Nederlandsche Bank (DNB).

DNB has created a good practice on information security. This good practice also offers a lot of useful insights into how to govern the CIA-triad (Confidentiality, Integrity and Availability) of data. Confidentiality is about protecting sensitive data from illegal access. Integrity concerns unauthorized changes in information systems where information must be kept intact and valid. Availability is concerned with data being available as well as accessible at all times (Warkentin & Orgeron, 2020). It offers a risk management cycle approach, next to a maturity assessment to be used by all types of organizations. Next to this, it also offers ways how to govern information security, how to deal with other organizations in combination with information security and outsourcing, among other components (De Nederlandsche Bank, 2023).

3.1.5.1 Testing the current state: maturity

Testing the current state of an implemented aspect within an organization is important to know how and where to improve. The current level of a certain element, such as the current level of cybersecurity preparedness, is called maturity. Measuring the maturity of a certain element within an organization may be hard if no measurable data is present. Maturity can be defined in several ways. Maier et al. (2012) define maturity as "*the state of being complete, perfect or ready*" (Maier, et al., 2012, p. 145). Maturity could also be defined as "*something or someone having reached the state of completeness*" (Maier, et al., 2012, p. 145). When a certain level of maturity is met, an organization may choose to maintain this level or to improve it even further up until a desired level.

3.1.5.2 Testing the current state: CMM model

Throughout history, there have been several models to measure maturity, for example the cybersecurity infrastructure of an organization. One example of this is the Capability Maturity Model (CMM). The model originally presents five maturity levels for measuring an organization's software process as well as for evaluating the capabilities of these processes. There is also a very similar model called CMMI, where the 'i' stands for integration. The model also helps to prioritize an organization's improvement efforts (GRC International Group, n.d.). However, this model may be biased in measuring knowledge management maturity within organizations. Krüger and Johnson (2010) found indications that the model has a tendency to favor endeavors in Information Management (IM), directly supported by Information and Communications Technology (ICT), above endeavors that require human intervention and/or a human component to succeed. Therefore, the assessment of the maturity of a specific part of an organization is not easily done, and needs complementary models to properly assess certain parts such as current cybersecurity maturity levels.

3.1.6 Overview of presented frameworks and standards

Bailey and Becker (2014) have looked into the similarities and differences of some of the presented frameworks, such as COSO, ISO 27001, ITIL, and COBIT. This overview clearly shows the overlap which became visible in the previous paragraphs. This overview is partly used in determining which frameworks are going to be used for the creation of the NIS2 framework. It looks as follows:

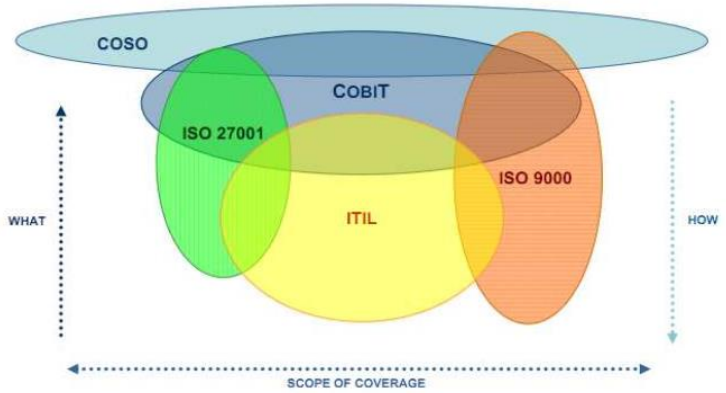


Figure 1: Framework relationships (Nguyen, 2010)

Figure 2: Similarities among different IT audit frameworks (Bailey & Becker, 2014)

Only a few of the above mentioned frameworks and maturity assessment models are useful for developing a NIS2 framework. This is due to limitations of the frameworks and maturity assessment models. ISO/IEC 27001 for example, should be regarded as the most important framework which is the closest to NIS2, since it specifically applies to cybersecurity. But since the scope of the research is only on the healthcare sector, NEN 7510 is more relevant. NEN 7510 is built upon ISO/IEC 27001, which means that the elements of the framework are still taken into account, but this is done by using a more relevant framework.

Framework	Use for NIS2 framework	Explanation
ISO/IEC/NEN	Yes	NEN7510 is the cybersecurity standard for the healthcare sector in the Netherlands. By comparing what parts are overlapping with the requirements of NIS2, the gap healthcare organizations still have to adapt will become visible.
COBIT	Yes	COBIT is one of the most important frameworks used in the auditing profession. It is therefore crucial to derive important elements for a NIS2 framework.
ITIL	No	The ITIL framework focuses more on the service elements of infrastructures and IT operations of organizations. This makes that ITIL is less suited to derive elements from for a NIS2 framework.

NIST	Yes	NIST focuses on information security and privacy management. Since it was developed by governmental institutions and different industries, useful parts can be derived for a NIS2 framework.
COSO	Yes	COSO focuses on Enterprise Risk Management by presenting controls. Since NIS2 prescribes steps to be done in order to comply, this can be compared with which COSO controls are already present in healthcare organizations.

Figure 3: Overview of to be used frameworks for the creation of a NIS2 framework

3.2 Compliance

Compliance is related to legislations and mandatory tasks to be done. McIntosh et al. (2023) define compliance as it involving adhering to legal and regulatory requirements, for example by organizations in Europe to ensure compliance with the General Data Protection Regulation (GDPR). In order to become compliant, an organization has to measure where they are currently. This is done by measuring the maturity of a certain element in the organization, as mentioned in section 3.1.5.1. Compliance can also be defined in an organizational setting, where employees have to comply to certain policies, such as information security policies. The use of this would be to gain success in information security. This can be done by having organizations invest into both socio-organizational and technical resources. This is important, because throughout the years it has not only be shown that the number of incidents related to information security is rising, but this is happening despite organizations investing in more technology-based solutions (Bulgurcu et al., 2010).

Despite setting up policies within organizations and the EU making the NIS2 directive obligatory for its member nations, the implementation and especially the compliance to them has differed severely. Bulgurcu et al. (2010) state that creating guidelines and policies is an essential starting point for compliance. It may not be enough to ensure full compliance, especially within organizations. This is exactly the case with the NIS2 directive which does not offer clear controls to be implemented. The same authors have looked into how information security awareness is influenced by information security policy, among various other mediators such as sanctions, rewards, perceived benefits of compliance, attitude and work impediments. The study shows that employees perceive work impediments to be costly. Organizations should therefore set aside an amount of employees' time to dedicate to fulfil the requirements of the created information security policy. Another finding shows that employee's self-efficacy regarding compliance positively influences the intention to comply. This suggests that organizations should train their employees. This way, employees know what to do in order to comply with the policy (Bulgurcu et al., 2010).

Constantly being remembered to comply to information security policies, may become demanding (for employees of an organization for example) in the long run. Cram et al.

(2020) looked into the concept of information security fatigue. Information security fatigue may occur when employees may become worn out by the many obligations and tasks by complying to the information security policy of an organization. Examples are having to change passwords every ninety days in combination with receiving frequent emails about not opening potential phishing emails, in combination with also having to take regular security trainings. The authors suggest that managers are better off with a more nuanced and targeted approach towards information security policy compliance. Less is more in this example in many cases. As security policy requirements are increasingly perceived as inconvenient and illegitimate, it may contribute to more security policy violations rather than less. More recently, Reeves et al. (2023) have developed the Cybersecurity Advice Fatigue Scale (CAFS), which measures (by conducting self-reports) the results from poor cybersecurity advice. They build upon the theory presented by Cram et al. (2020). Reeves et al. (2023) suggest that creators of cybersecurity trainings should review their content. Specifically, they should look into existing knowledge of their audience whether the created content will match with the preferences of the audience, whether the intent behind the content is clear and which emotional responses may be triggered by the training. Since management training is new with the launch of NIS2, this needs to be taken into account when trainings for management are created.

3.3 Healthcare

Healthcare providers have become one of the most popular targets in the healthcare sector throughout the last few years (Almulihi et al., 2022). Examples of this are the high worth of patient data in the black market. An example is that a full set of medical credentials can cost up to €1000 on the black market (Sushma et al., 2023). There are different organizations within the healthcare sector. According to NIS2, a healthcare provider means "*any natural or legal person or any other entity legally providing healthcare on the territory of a Member State (of the EU)*" (European Parliament, 2022, p. 66). Examples of healthcare providers include hospitals, general practitioners (GP), reference laboratories, entities researching and developing medicinal products, entities manufacturing (basic) pharmaceutical products, and entities manufacturing medical devices considered to be critical during a public health emergency (European Parliament, 2022).

Healthcare can be divided into several categories. According to the Central Agency of Statistics (CBS), these categories are university medical centers, hospitals and other medically specialistic health, mental health, General Practitioners (GPs) and health centers, other health and welfare, nursing, care and home care, disability care, youth services, social work and childcare (Centraal Bureau voor de Statistiek, n.d.).

An important and big part of decision making within organizations generally is done by the Board of Directors (BoDs). Throughout the years, Enterprise Risk Management (ERM) has become one of the most important parts to govern within an organization. The BoDs are also accountable for regulatory compliance and the oversight of the financial performance of the organization. Throughout the years, cybersecurity risk management has been rising quickly to the main priorities of the BoDs (Bongiovanni et al., 2022). This is shown even further with new regulations such as NIS2 which holds natural persons accountable for organizations accountable for failing to take these topics to the agenda of the BoDs and to improve the current cybersecurity infrastructure. BoDs have been called upon into taking a more centralized role in governing their organization, which is visible in NIS2 with the mandatory training for management regarding cybersecurity risks. Managing Confidentiality, Integrity and Availability (The CIA-triad) has become a major risk for organizations (Scully, 2014). Therefore, a framework how to deal with this needs to be utilized.

CIOs rarely report to CEOs, and CIOs are often not board members (Grobman & Cerra, 2016). This makes that there is a lack of ways how to measure and assess cyber security investments. Next to this, cybersecurity is perceived as too technical for BoDs. Since the engagement with cybersecurity is only going to get more, it is necessary to have cybersecurity training for directors (Bongiovanni et al., 2022). Within hospitals, the BoDs and decision-makers not only need to talk and make decisions about cybersecurity (because of directives such as NIS2 and because they can be held accountable if they fail to implement such directives), but also need to understand the current cybersecurity risks and challenges. Frameworks can help with this.

Challenges in cybersecurity in healthcare organizations are ransomware attacks, (email) phishing attacks, misplacement or unauthorized acquisition of equipment or data, data loss caused by insiders (either on purpose or accidental), and attacks on devices that are connected in the organization that may affect the safety of patients (Sushma et al., 2023). Since NIS2 also highlights awareness training, this needs to be taken into account when controls in a framework are created.

With new advancements and new ways how to utilize new technologies in the healthcare sector, it is critical that cybersecurity gets prioritized (Tarikere et al., 2021). One example of this is weak authentication methods for medical devices, which increases security concerns such as cyber-attacks and data theft (Arfaoui et al., 2019). Despite new advancements in technologies and applications, the healthcare sector still suffers from technical vulnerabilities. This is due to advancements in ways how cyberattacks are executed (Mamdouh et al., 2021).

Next to this, further enhancements in regulatory guidance to mitigate risks are needed. Examples of this are old IT infrastructures being built into medical devices, edge-to-cloud interfaces, and off-the-shelf components for the device (Thomasian & Adashi, 2021).

Healthcare applications or medical devices often use outdated technology, such as old soft- and hardware. This is of good use to a hacker, which can easily manipulate this to get access to sensitive data. Medical devices are often not designed with the intention against security attacks, but just for medical assistance. This can also lead to easy access to the device. The problem with this is twofold; not only can data be stolen, but a patient could get in trouble if the machine is hacked and the patients' health relies on the device (Sushma et al., 2023).

Healthcare practitioners can lessen the chance of unauthorized access to healthcare data by nursing employees. This can be done by developing and planning training programs for employees. Examples of this are privacy-preserving behavior, which has been shown as one of the essential means for ensuring a proper practical implementation of ethical norms in practice (Mikuletič et al., 2024). Creating a strong security culture in the entire organization is key for successful cybersecurity awareness and knowledge of employees. Creators of the trainings and/or security programs should be very mindful with the various group dynamics and possible existing subcultures of organizations to encourage socialization. This will help with implementing the desired security knowledge (Tejay & Mohammed, 2023).

Most organizations use a linear incident response framework to prevent, detect, contain, eradicate and learn lessons from incidents. However, due to the robustness of this approach, it may turn out to be ineffective (He et al., 2022). Therefore, new ways of dealing with cybersecurity risks need to be implemented. Next to this, the size of a healthcare organization such as a hospital could mean different levels of risks are associated with them, where a large hospital is targeted by hackers more quickly than smaller hospitals (McLeod & Dolezel, 2018).

Outsourcing some of the cybersecurity risks is another topic that comes with dealing with cybersecurity risk management. Outsourcing responsibilities is never the way to go however (Leino, 2024). Cascavilla (2023) also predicted that cybersecurity insurances may even become illegal in the upcoming years, where the push for preventative measures will become obligatory. Based on a risk-assessment matrix/heatmap, the size of the impact of a possible cybersecurity incident and the actual probability that the incident might happen can be plotted. An example is presented in appendix 3. If an identified cybersecurity incident is in the high/high corner, direct measures need to be taken. If a possible incident is in one of the high/low or low/high corners, self-insurance can be done to reduce the possibility of the incident to occur. This can be done by investing in cyber technology tools which help decreasing the probability of the incident

to occur. Next to this, a contingency fund to make good the loss from an incident if it were to happen should also be created (Mukhopadhyay & Jain, 2024).

The healthcare sector is one of the essential organizations within NIS2. Sufficient cybersecurity is key to maintaining daily operations within a hospital. According to Roodhooft (2024), the three key priorities for healthcare cybersecurity leaders are 1) securing internet of medical things (IoMT) devices, 2) leveraging automation and Artificial Intelligence (AI), and 3) managing regulatory compliance (Roodhooft, 2024). Compliance to new regulations has proved itself to be increasingly more difficult, especially with the obligation to document more and more (such as the reporting obligation presented in NIS2).

An example of how other countries deal with the coming of NIS2, is the example of Belgium. In Belgium, hospitals were not under the scope of NIS1. This is different from the Netherlands, where hospitals did fall under NIS1. This means that Belgian hospitals did not have to report security incidents, where Dutch hospitals did have to report incidents. With NIS2, this changes. The AZ Vesalius hospital is a leading hospital in Belgium. Roodhooft (2024) presents that the AZ Vesalius hospital will prepare for NIS2 by obtaining an ISO27001 certification. The ISO27001 certification helps organizations set up specifications for an effective information security management system (ISMS).

3.4 Cybersecurity

Implemented cybersecurity countermeasures that seemed to be promising at the time of implementing them prove themselves to be less effective over time within organizations. This may stem from the perceived cost of the (initial) cost of behavior change for employees, and the (difficulty of) building habits. A specific example of this when a sanction is present when a violation of a certain cybersecurity policy is broken. The initial sanction may be effective at encouraging compliance at the start. This may change as employees have more time to take a second look at the situation, when they reappraise the situational factors surrounding them. Thinking about the likelihood of getting caught for violation means that the influence of the initially created sanctions becomes weaker as time passes. Even though cybersecurity controls stay the same, it could be that the affective factors and emotions of employees become stronger predictors of compliance over time. Managers can leverage this to implement more effective techniques. The authors also mention cybersecurity fatigue as an important factor to take into account to make sure that compliance goals are met, as mentioned in the previous paragraph (Cram et al., 2024).

3.4.1 The application landscape in the healthcare sector

Within the healthcare sector, several types of applications are used for different purposes. This makes for a complicated application landscape (Tin et al., 2023). There are applications which are being sold to healthcare institutions by manufacturers which run on medical devices, for example. Other examples are applications in which data of patients is being used, which often store and process very sensitive data. Within healthcare, the most commonly used applications are the Electronic Client Record (ECR) or Electronic Patient Record (EPR). In the Netherlands, they are not called a record, but a dossier. Therefore, the used synonyms are Electronic Client Dossier (ECD) for clients, and Electronic Patient Dossier (EPD) for patients. Therefore, the terms ECD and EPD will be used from now on.

EMRs are digital versions of paper charts that are used by healthcare professionals, which are highly specified to a patient's medical history in a specific area of healthcare. EMRs don't easily transfer out of one area of healthcare, which means that physically printing them out (and sending them to the designated person) is often the only solution (Fu, 2022).

ECD is a tool to keep track of data for the long term. EPD stores more detailed data, which is more targeted towards the 'cure' sector (hospitals and GPs). EPD's main goal is to find a lot of information on patients to share with colleagues (Cliendo, 2023).

The infrastructure of healthcare organizations is very broad, since it has to communicate with different partners. An EPD is not only used to share data within the organization, but also with partners. An example of sharing data outside the organization is a health insurer, which needs to process the information.

BDO audits several health applications in the healthcare sector by executing IT-audits. BDO has therefore a good overview of the currently most used and important healthcare applications in the field. A few of these applications are ONS from the organization Nedap, Ysis by Gerimedica, and PUUR. which is owned by the organization Ecare. Nedap also offers other applications such as the mediKIT application, which is a GP information system which supports the daily activities of GPs. It also helps to make the correct choices to ensure a sufficient health quality. Collaboration among the GP health service is smoothened as well. Data can be inserted in an easy way, which will become visible to be used for making decisions and creating and updating policies (Nedap, 2023). Despite advantages of sharing data easily between different parties, a lot of risks come with handling sensitive data. It is therefore important that organizations which collaborate with healthcare providers, are also aware of NIS2 and their role, since (data) incidents can occur despite the healthcare providers being fully prepared to prevent any incident. If partners of healthcare providers do not take NIS2 into account, or only in a limited way, collaborating with these partners may become very difficult in the future. This is

not only due to the fact that sensitive patient data is being handled, but also because of the fact that an incident involving this sensitive patient data may come from the network of the healthcare provider. Partners of healthcare providers which offer healthcare solutions have to be assessed properly in the process of becoming NIS2 compliant. Potential new partners will have to be found if the current partners do not prove themselves to be NIS2 compliant (or if they will not become compliant any time soon).

3.4.2 Application landscape risks

With all these systems and interdependencies among these systems, a lot of risks come with handling the use of the systems. This comes in both the data being used and processed by humans, as well as by risks of data being shared from one application to another. Khansa et al. (2012) mentioned that the healthcare landscape has become a more integrated, interoperable platform, which is used for the communication, processing, storing and accessing health data and knowledge. Moving into the age of EMRs, new security measures are necessary.

The supply chain of information entails information being send to other organizations, or information being received from another organization. This means that a healthcare organization can protect its IT infrastructure in the best possible way, and still become victim of a cybersecurity incident which took place at one of the partner organizations. Van Der Meulen (2013) gives the example of municipalities relying on governmental services and websites. Governmental services form a crucial link for residents of the nation. If this service is down, this may have major implications for the day-to-day activities of all residents of a nation. A comparable situation can occur if a partner organization of a healthcare organization, such as a hospital, gets hacked or is unavailable. This could potentially mean the difference between life and death in certain situations.

When patient data is stolen, the data and the identities of patients can be stolen and even sold on alternative marketplaces. This is a problem, since not many organizations in the healthcare industry are not updating or even keeping track of all the potential as well as known risks and elements into a centralized database. If an analysis were to be made, this would benefit both the healthcare organization as well as the auditing authorities and insurance organizations (Schmeelk, 2022). The complexity of the application landscape, combined with the increasingly higher risk of data breaches in the healthcare sector compared to any other sector (Tin et al., 2023), make that a proper analysis of risks is needed. Tin et al. (2023) broke down seven types of primary categories of data breaches within hospitals. The biggest categories were hacking/IT incidents, theft, loss, improper disposal, and unauthorized access or disclosure.

Schmeelk et al. (2021) present an overview of types of data breaches in the time period of May 2018 to May 2019 based on the US HHS OCR Breach Portal. Despite the results presented in the report were only self-reported incidents, it still gives a good indication of the ways how data breaches occurred. The most data breaches occurred via the following ways (in order): email, paper/films, network servers, desktop computers, laptops, and electronic medical records (of patients).

3.5 Conclusion literature review

Compliance has been shown to be a difficult topic, even within different sectors and different types of organizations. Cybersecurity compliance has proved itself to not only be crucial with the ever-increasing threats to more and more types of organizations. Assessing the current status of cybersecurity implementations, such as risk management procedures, helps with working towards a new level of maturity. But this cannot be done without the help of proper frameworks to guide organizations. Within the healthcare sector, NEN 7510 is the most important framework. This framework is based on ISO/IEC 27001. NEN 7510 focuses more on the data of patients, rather than the data of every natural person involved with the organization. It is therefore crucial to compare NEN 7510 with the requirements of complying with NIS2.

In order to create a sufficient framework to comply with NIS2, assessment of the current status of the healthcare sector is important prior to starting to change and improve certain cybersecurity elements. The frameworks COBIT, NIST, and COSO have been shown to be useful to develop a NIS2 framework. The same applies to the good practice on information security by DNB. These frameworks and guidelines will be discussed in detail in chapter 5.

4 Theoretical background (methodology)

A Design Science approach will be used to create a new framework. The developed framework will come from the literature review, the NIS2 in context chapter and the reviewed (in-depth) research about useful currently available frameworks. Hevner et al. (2004) came up with the grid to fill in for design science research. Each block represents a part of the design science research process. Since each research project is different, it must be altered to the needs of each individual research project. The original model by Hevner et al. (2004) is shown below:

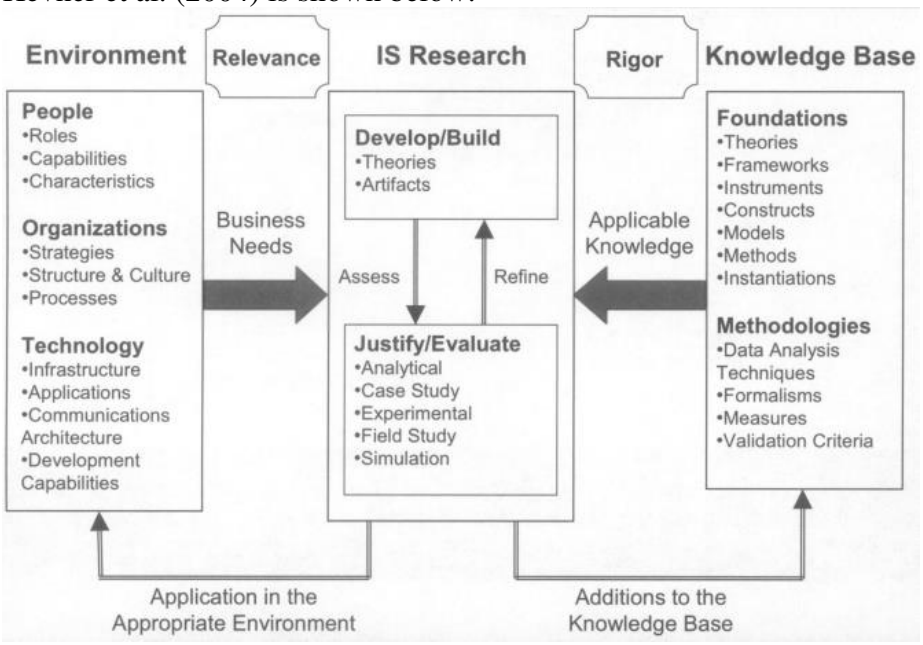


Figure 4: Hevner et al. (2004) on how to conduct design science research (with elements).

Since NIS2 is a new directive coming from the EU which has to be translated into local laws by the Dutch Government, a lot of legal knowledge is required to gather. As Hevner et al. (2004) state, this is part of the knowledge base. The knowledge base is translated into the NIS2 in context chapter (chapter 2). The knowledge base will consist of both the foundation and different methodologies which are used within the research.

It is important to have different (already useful) frameworks analyzed to use (parts) of them to create a NIS2 framework. Next to this, knowledge centered around NIS2 (legal documentation) is needed to create a foundation of the current status of NIS2 in the Netherlands. A literature review as well as expert interviews will be conducted for researching the research question, as stated in paragraph 1.2. This is the methodologies part of the Hevner et al. (2004) framework. The framework will thus be created from the foundation part (current useful frameworks, NIS2 legal documents), the literature review and the expert interviews to update the framework. When these parts are done, the framework will be verified by two healthcare experts, where the framework can be checked in practice. This will be done within BDO, where documents of partner

organizations of BDO can be used. This will be done by using the IT audit protocol 'Cyber in the audit' used within BDO. The consulted people for the expert interviews are IT auditors, cybersecurity consultants and advisors, and IT consultants. The applicable organizations are all types of health(care) organizations within BDO's network (scope) that must comply with NIS2, as well as BDO itself. There is no technology present, since technology is often used in technical settings, which the creation of a framework is not. Below, an overview of the applied Hevner et al. (2004) framework for this research project is presented.

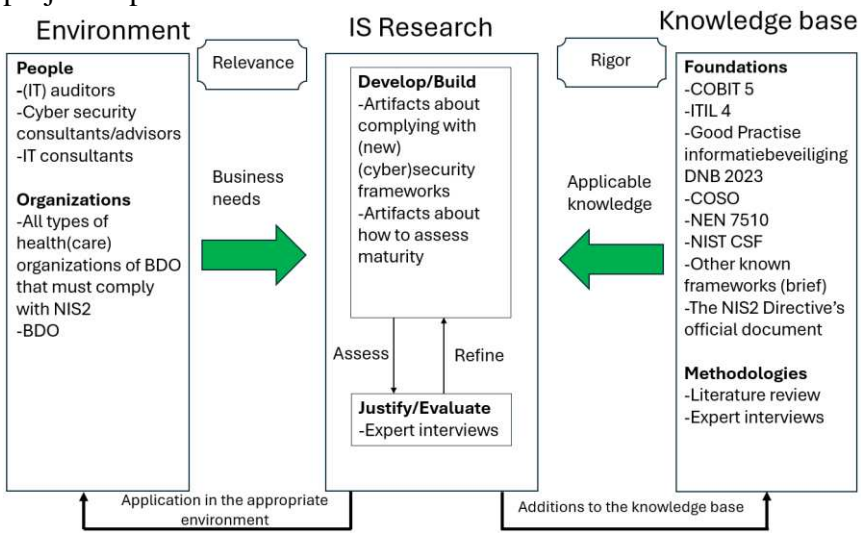


Figure 5: Filled-in Hevner et al. (2004) framework on Design Science for this research.

4.1 Selection of methodology

The framework will be created based on the NIS2 in context chapter, the literature review, and the reviewed parts of other useful frameworks, which are COBIT, COSO, the Good Practice on Information Security by the De Nederlandsche Bank, The NIST Cybersecurity framework (SCF), and NEN 7510. After this, semi-structured (expert) interviews will be held to verify the created framework. Then, the framework is validated with experts within the healthcare/cybersecurity field by using the IT audit check 'cyber in the audit'[8]. These will be internal experts within BDO with a minimum experience level of junior manager.

4.1.1 Research setup: pilot interviews

The interviews described in the design science approach will be designed so that different levels of experience will be examined. First, two pilot interview regarding the importance of parts of NIS2 will be examined. According to Turner (2010), a pilot test

[8] Cyber in the audit is part of certain IT audits done within BDO, which specifically focus on cybersecurity measures and controls.

should be implemented to assist the research in determining if there are any flows. It should be conducted with participants that have similar interests (or expertise) as those that will participate in the final study. This will be done by asking Junior IT auditors within BDO about their perception of which parts of ITIL and COBIT should be important and placed in a NIS2 framework. The results of the interview will be compared with the literature review where it is assessed which parts of these current frameworks are considered important. Next to this, the in-depth interview protocols will be created with the pilot interviews kept in mind.

Before the pilot interviews are conducted, an email which contains a link to a survey regarding the importance of certain constructs of which a proper framework should consist of will be send. On a 5-point Likert scale, respondents are asked about the importance of certain things within the created framework. The scale will range from not important to very important. Prior to the actual pilot interview itself, the responses from the asked questions will be looked at. This way, comparing the results with the literature review where the most important constructs from already consisting frameworks can be done.

It is deliberately chosen to interview two junior IT Auditors, so that the interview protocols can be created and used for 'more experienced' IT auditors within BDO. This way, the interviews are tested, and the interview setup can be improved so that the 'real' interviews will go as smoothly as possible. The pilot interview setup can be found in appendix 23.

4.1.2 Research setup: in-depth interviews

For the in-depth interviews, several respondents will be selected within BDO. The focus will be on the more 'experienced' level of IT auditors, (junior) managers and partners. These people have a lot of experience, and are therefore better able to critically assess the initial NIS2 framework based on the literature review. They must have at least four years of considerable experience in the cybersecurity or healthcare legislation field. All interviews will be anonymized. Appendix 22 presents the list of interviewed experts within BDO, as well as if they were interviewed for the second or third iteration of the framework. Appendix 24 presents the interview protocol for the validation interviews.

A standardized interview setup will be used. The questions are the same for every respondent. However, a semi-structured interview will be used, so that respondents can be asked in more detail why they think that a certain construct is more important than others. According to Adams (2015), using semi-structured interviews is very useful if one needs to conduct an evaluation of a (formative) program, especially where one-on-one interviews are needed with people which have key experience for the subject one is

interviewing them about. This way, updating the NIS2 framework is done in a sufficient manner, based on the surveys and interviews.

Coker (2023) looked into triangulation in combination with reliability and validity of dissertations. Using data of different types (in this case, both interviews for verifying the framework and then validating the updated framework afterwards) are able to help to determine not only the interpretations of certain phenomena, but also with providing complementary information about the studied subject.

4.2 Data collection and analysis (knowledge base)

Since in-depth, (open-ended) interviews will be used as well as written documents, a qualitative research study fits better than a quantitative one (Patton, 2005). A qualitative study generates rich narrative descriptions, which fits with the development of a new framework.

By using several ways to research the identified problem, several methods are used. Brewer and Hunter (2006) state that by using a 'multi-method approach' the quality of the research increases, which adds more value to the developed framework.

Informants are selected via the internal network of BDO. Email and the intranet of BDO will be used for this, as well as consultation from the thesis supervisor within BDO.

The results are analyzed by comparing the collected data from the interviews, and then comparing the most common results with the parts which the literature has proved to be the most important for the NIS2 framework. Analysis of the interviews will be done via color coding: each element of the framework which is discussed will receive a specific color, as presented in appendix 21. The initial framework will be updated accordingly, after enough respondents have been consulted. The number of respondents to be used for the interviews will be based on the concept of data saturation. Data saturation is defined as the amount of gathered data (in this case: interviews) when there is enough information to replicate a study, when the gathering of additional information and coding is no longer feasible. Sufficient data saturation will also improve the validity of the research by triangulation (Fusch & Ness, 2015). In practice, this means that when interviewees respond in a similar fashion to the standardized set of answers, the point of data saturation is reached: "*If one has reached the point of no new data, one has also most likely reached the point of no new themes; therefore, one has reached data saturation*" (Fusch & Ness, 2015, p. 6). Since this scope of the research is NIS2 in the healthcare sector, which is substantially smaller than all sectors within NIS2, the point of data saturation will be reached faster: "*a small study will reach saturation more rapidly than a larger study*" (Fusch & Ness, 2015, p. 4). The most commonly mentioned feedback will be used as a starting point and validation of the created framework. The answers will be anonymously integrated in the thesis.

Finally, internal documents will be used to improve the framework even more, together with documents from official sources. Examples of this are the EU or instances which have audited similar (cyber)security legislation in the past, or processes which helped organizations to comply to new regulations.

4.3 Description of empirical data (IS research, environment)

For the literature review, mostly top IM-journals are used. The complete list of journals can be found in appendix 2. The used database for the keyword search will be done on ScienceDirect. At least three different journals which have been listed as useful by the above mentioned list have to be consulted. Next to this, other useful journals with neighboring fields may also be consulted. The used timeframe is 2014-2024 (ten years), because the field has changed over time. Therefore, older sources may not be as useful. If older sources turn out to be useful, they will be used and cited in the newer papers. The used article types are research articles and review articles. The used subject areas are Business, Management and Accounting (1) and Computer Science (2).

By using Tilburg University's Business Source Ultimate database for finding papers, a few sector specific papers have been found, however. This was done by specifying the keyword "NIS2" and the timeframe "2022-2024". They specialize around healthcare, energy & (drinking) water, and pharmacies. Since the scope of the research is on healthcare, energy & drinking water will be skipped.

In the following table, an overview of the results of the keyword search query on ScienceDirect has been presented (as per February 2024). The potential useable papers are determined based on the names of the journals. If they are in the listed top journals according to Tilburg University or in a neighboring field, they are considered as potentially useful. If papers from top-journals are presented in one of these papers, they may be used as well. It should be noted that cybersecurity is often used interchangeably with the term "information security". However, in recent years, the term cybersecurity has seen an increase in popularity (Cram et al., 2024). The results are as follows:

Keyword combination	Amount of results	Potentially usable papers
"maturity assessment" "legislation"	25	19
"healthcare", "compliance" and "cybersecurity"	550	292

Table 3: Overview of potentially useful papers for the literature review

The data being collected will be mainly about (cyber)security frameworks, and specifically the parts which will be useful for the creation of a new NIS2-framework. Organizations can be assessed so that they know where to improve to comply with NIS2.

By creating a framework based on a literature review as well as consulting experts on this topic, the framework will become more mature over time.

4.4 Reliability & validity

Reliability refers to the degree to which multiple measurements within an executed research give the same result. Validity refers to the degree to which the scores on a measure represent the things they are intended to (Van Der Vliet, 2022). Reliability and validity can be demonstrated in various ways. Since a design science approach is used in the creation of a new framework, only a few methods of demonstrating reliability and validity are applicable.

4.4.1 Reliability

Reliability of the research can be demonstrated by examining the process how the data was collected and kept (Lincoln & Guba, 1985). This refers to the accuracy of the collected data. Reliability has therefore to do with the interviews to improve and validate the created NIS2 framework, as well as with the collected information in both the NIS2 in context chapter and the literature review on NIS2.

The reliability in the research for the NIS2 in context chapter and literature review is demonstrated by the collection and combining of different sources regarding NIS2. All sources are either coming from official sources from either governmental institutions within the Netherlands or the European Union. For the literature review, all sources can be traced back and read to confirm the presented information.

4.4.2 Validity

Larsen et al. (2020) have created design science validities, which are the most common ways to validate design science research. Design science validities are defined as "*formalized procedures for justifying arguments and conclusions of a research study involving the design, development and/or evaluation of IT artifacts to solve identified problems*" (Larsen et al., 2020, p. 276). The most used types of validities are criterion validities, where accuracy and recall are the most often used types. Then, internal design validities are the most used, which are used to reflect the desire of the creator of the research to attest the internal qualities of a framework. The most used internal validity type is consistency (Larsen et al., 2020). Since the framework will only be tested and validated internally, the validity of the research will not be as high as the internal validity.

4.4.2.1 Internal validity

Because the framework is tested internally within BDO, internal validity can be demonstrated. Larsen et al. (2020) state that a created framework is often evaluated against an external criterion. In the case of this research, this will be done by the expert interviews to improve the framework. Validating the created framework will also be done by consulting internal cybersecurity specialists within BDO.

Lincoln and Guba (1985) have created different criteria with subsequent techniques to demonstrate different types of reliability or validity[9]. For internal validity, there are seven techniques which can be used. For this research, only three techniques are relevant. These are triangulation (already mentioned in the research design), member checks (verifying the framework by experts), and referential adequacy (literature review & NIS2 in context chapter). By using these three techniques, internal validity can be demonstrated.

4.4.2.2 External validity

External validity refers to "*the extent to which causal knowledge can persist over variation in persons and treatment settings*" (Averitt et al., 2021, p. 1). In terms of a framework creation, external validity refers to the generalization of the framework (Andrade, 2018). Because there is no random sampling done within the creation and validation of the framework, the results may not be generalized to other contexts. If all sectors within NIS2 were to be taken into the scope of the research, and methods such as random sampling were used, the framework could be generalized in some way. Since this is not the case, the external validity of this research is quite poor.

[9] See appendix 4 for an overview of all methods to demonstrate reliability and validity.

5 Current framework analysis

For the creation of the NIS2 framework, five frameworks will be used. They are COBIT, COSO, NIST, NEN 7510, and the Good Practice on Information Security by De Nederlandsche Bank. Each framework presents useful elements to be used for the creation of the NIS2 framework.

Each framework will be compared with NIS2. For example, COSO will look into Risk Management. For that topic, based on the NIS2 in context chapter and literature review, the measures presented by COSO to work out the obligations which are mentioned in NIS2 are presented.

5.1 COBIT 5

COBIT is one of the most known and used frameworks (ISACA, n.d.). It is built upon five key principles for managing enterprise IT and governance. This is summarized in the following table:

Principle name	Summary
Meeting stakeholder needs	Enterprises have to create value for their customers, as well as for their stakeholders. This can be done by maintaining a balance between the use of resources and the optimization of risks, and the realization of benefits. COBIT provides organizations with all the required enablers and processes, to support the creation of value through the use of IT.
Covering the enterprise end-to-end	The governance of enterprise IT is seen as general governance of the entire organization. It focuses not only on the IT functioning of the organization, but also on information and related technologies. COBIT treats information and related technologies as assets which need to be dealt with in a similar way as with any other asset within an organization. COBIT considers all management enablers as well as all IT-related governance to be an enterprise wide and end-to-end.
Applying a single, integrated framework	COBIT aligns with current frameworks and standards to create a single, integrated framework which is useful for all types of organizations. COBIT can therefore be used as an enterprise-wide framework for the management of enterprise level IT and governance.
Enabling a holistic approach	Having efficient and effective governance as well as management of enterprise level IT requires a holistic approach. This approach should take different types interacting components into account. COBIT defines a set of enablers for the support implementing an extensive management and governance system for enterprise level IT. Enablers are broadly defined as "*anything that can help to achieve the objectives of the enterprise*" (ISACA, 2012b, p. 14). COBIT defines seven categories of enablers. These seven enablers are worked out in appendices 5 to 11.
Separating governance from management	COBIT makes a very clear difference between management and governance since governance and management encompasses different types of activities. COBIT's view on the key differences between governance and management is mainly focused on the differences of responsibilities. Overall governance of an organization is often the responsibility of the BoDs, and specific

	governance is often the responsibility of special organizational structures. Management is often the responsibility of the executive management.

Table 4: COBIT 5's five principles summarized (ISACA, 2012b).

5.1.1 Relation COBIT to other frameworks

COBIT is related to other frameworks. The standards which are implemented within COBIT are ITIL, the ISO/IEC 27000, 20000 and 31000 series, TOGAF, CMMI, and PRINCE/PMBOK.

ITIL and ISO/IEC 20000 cover parts of the DSS, BAI and APO domains. The ISO/IEC 27000 series covers the EDM, APO, DSS and MEA domains. ISO/IEC 31000 covers the EDM and APO domains. TOGAF covers the ADM and APO domains. CMMI covers the BAI and APO domains. PRINCE2 coves the APO and BAI domains. An overview of this is covered below:

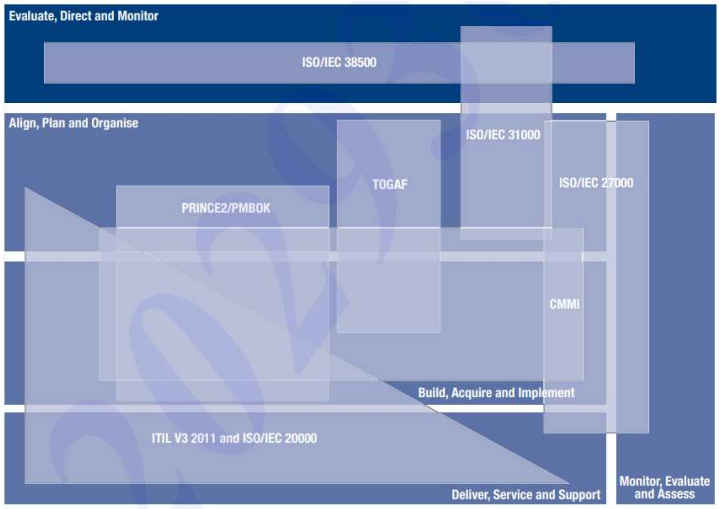


Figure 6: COBIT's coverage of other standards and frameworks (ISACA, 2012b).

5.2 COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has created a worldwide accepted framework to manage risks. COSO calls this the Enterprise Risk Management (ERM) – integrated framework. The title is ERM – aligning risks with strategy and performance. The framework itself is composed of a set of principles, divided into five interrelated parts (Committee of Sponsoring Organizations of the Treadway Commission, 2016). This is visualized below.

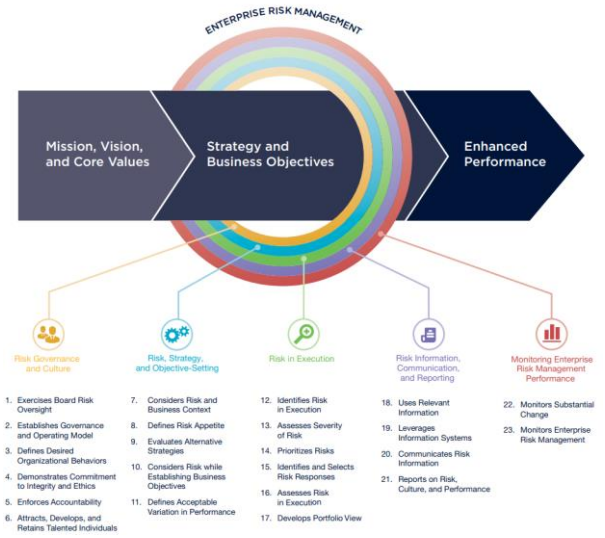


Figure 7: COSO's ERM framework (Committee of Sponsoring Organizations of the Treadway Commission, 2016).

The five sets of principles are summarized in the table below.

Principle name	Summary
Risk governance and culture	The main purpose is to set the organization's tone regarding ERM, as well as creating oversight responsibilities, and reinforcing the importance of ERM. The culture part refers to the ethical values organizations have in place, as well as the desired behavior from their employees.
Risk, strategy, and objective-setting	ERM, the setting of objectives and strategy are aligned in the process of strategic planning. The amount of risk an organization takes is described as their "risk appetite". This appetite should be aligned with the created strategy of an organization. Business objectives put the strategy into reality, and serves as a baseline for the process of identifying, assessing and responding correctly to risks.
Risk in execution	Refers to risks which may have an impact on achieving the strategy and business objectives. The identified risks have to be prioritized based on severity, while keeping the risk appetite of an organization in mind.
Risk information, communication, and reporting	ERM requires a process which is about sharing and obtaining information. This process is continuous, and relates to both internal and external sources.
Monitoring ERM performance	Each organization can consider how sufficient the components of ERM are currently functioning. This can be monitored over time, as well as in the ways how changes are occurring

Table 5: COSO's five principles summarized (Committee of Sponsoring Organizations of the Treadway Commission, 2016).

5.3 NIST

NIST offers the Cybersecurity framework (CSF). The CSF offers guidance on cybersecurity to different industries, governmental agencies, and other types of organizations. The framework proposes outcomes by offering a taxonomy of high-level cybersecurity. The framework can therefore be applied to any type of organization, independent of the size, maturity level, or sector. The framework is not prescriptive, but it links to other useful sources to provide extra guidance on controls and practices

(National Institute of Standards and Technology, 2024). The framework is composed of five functions. These five functions are known as the Framework Core. The five functions consist of different categories and subcategories. References to other frameworks such COBIT and ISO are also made in the framework (Toussaint et al., 2024).

5.3.1 The different functions of the CSF

The CSF defines five functions, next to one generic function. These functions are Identify, Protect, Detect, Respond and Recover. The generic function is Govern (National Institute of Standards and Technology, 2024). These six functions are summarized in the table below.

Function name	Summary
Identify	Identifies and prioritized risks and assets of cybersecurity. The function also ensures that the current cybersecurity risks are understood. By understanding the assets of an organization, such as data, hardware, software, systems and people), as well as suppliers, organizations can prioritize its risk management strategies.
Protect	Helps organizations to manage cybersecurity risks by the help of safeguards. The function can help to support to secure assets, to decrease cybersecurity risks and to take advantage of opportunities. Results stemming from the protect function are identity management, access control, authentication, awareness and training, resilience of technology infrastructure, data security, and platform security.
Detect	Entails finding possible cybersecurity attacks and compromises. These findings are then analyzed. This function is about discovering threats and anomalies in a timely manner, as well as indicators of compromises and other potentially adverse activities regarding cybersecurity. The function supports the successful implementation of incident response as well as recovery activities.
Respond	Defines actions related to detected cybersecurity incidents. The function supports containing the possible adverse effects of cybersecurity incidents. Results of this function are incident management, mitigation, reporting, communication and analysis.
Recover	Makes sure that assets and operations which are affected by cybersecurity events are correctly and sufficiently restored. Restoring data must be time in in a timely manner, to reduce the effects of the incidents.
Govern	Entails governing the five functions of the CSF. It is visualized in the center of the CSF, because this generic function informs how organizations have to implement the five functions of the CSF. Offers solutions to inform what kind of prioritizations organizations may have to reach its desired outcomes, such as its mission. Activities regarding governance are essential for implementing a broader enterprise risk management (ERM) strategy, specifically tailored to cybersecurity. Addresses understanding of the organizational contexts within organizations.

Table 6: NIST's six functions summarized (National Institute of Standards and Technology, 2024).

5.3.2 Profiles of the CSF

The CSF presents two types of profiles for organizations. NIST presents this as organizational profiles, which are used to “understand, tailor, assess, prioritize, and communicate the Core’s outcomes by considering an organization’s mission objectives, stakeholder expectations, threat landscape, and requirements” (National Institute of Standards and Technology, 2024, p. 6). Every organizational profile includes either a

current profile, or a target profile. These profiles can be seen as the current core outcomes (current situation) and the target core outcomes (future situation).

There are five steps to go from a current to a target situation within the CSF. These steps should be repeated. The steps are visualized and explained below:

Figure 8: The steps for creating and using a CSF organizational profile (National Institute of Standards and Technology, 2024).

Step name	Explanation
Scope the organizational profile	Documentation of the high-level facts and assumptions related to the profile should be done.
Gather needed information	Examples of information are risk management priorities, organizational policies and cybersecurity requirements and standards to be followed within the organization.
Create the organizational profile	The types of information which should be included for the selected CSF outcomes have to be determined. Risk implications have to be considered to inform the target profile (the future situation).
Analyze gaps and create an action plan	A gap analysis has to be done to identify and analyze differences within the present and desired future situation. A prioritized action plan has to be developed after this. An action plan may entail a risk detail report or a risk register.
Implement action plan and update profile	Executing the action plan has to be done in this final step. There may be deadlines for the execution of the plan. The action plan can also be ongoing throughout improvement efforts.

Table 7: The five steps of the CSF (National Institute of Standards and Technology, 2024).

5.3.3 Tiers of the CSF

An organization can pick using tiers to inform the current and target profiles. Tiers are useful for categorizing the rigor of an organization's cybersecurity governance regarding risks and management practices. Tiers can provide context for how an organization views its identified cybersecurity risks, as well as the processes in place to manage these risks. The tiers reflect an organization's current implementations regarding managing cybersecurity risks. There are four tiers described in the CSF. These are 1) partial, 2) risk informed, 3) repeatable, and 4) adaptive. This is visualized below.

Figure 9: CSF's tier setup regarding managing cybersecurity risks (National Institute of Standards and Technology, 2024).

The tiers should complement an organization's risk management regarding cybersecurity, instead of replacing it. An example of this would be using the tiers to communicate internally via a benchmark. Progression to higher tiers is encouraged when certain identified risks become more likely to appear (National Institute of Standards and Technology, 2024).

5.3.4 Risk management within the CSF

There are three levels of organization-wide risk management approaches, which are organization, mission/business processes, and information system (National Institute of Standards and Technology, 2018). The SP 800-30 can also be used for this, which offers a guide for executing assessments of risks. The NIST Privacy Framework can be used to address and govern various aspects of both privacy and cybersecurity risks (National Institute of Standards and Technology, 2024).

Next to these guides to manage cybersecurity risks, the CSF explicitly mentions the differences and overlap between cybersecurity risks and privacy risks. They show that the cybersecurity related privacy events are overlapping both types of risks, which in turn require more attention (National Institute of Standards and Technology, 2024). This is shown visually below:

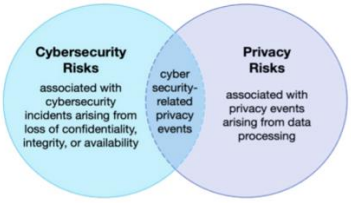


Figure 10: The overlap between cybersecurity and privacy risks (National Institute of Standards and Technology, 2024).

5.3.5 Supply chain cybersecurity risk management

The CSF of NIST refers to the cybersecurity supply chain risk management practices for systems and organizations. Supply chain risk management (SCRM) has always been important, but managing an entire supply chain proves to be even more difficult when it comes to cybersecurity. Cybersecurity SCRM (C-SCRM) is therefore a systematic process which helps with managing possible exposures to cybersecurity risks within supply chains. This can be done via the creation of sufficient response strategies, processes, policies, and procedures. The subcategories within the supply chain framework offers connections between focus on C-SCRM and outcomes based purely of cybersecurity (National Institute of Standards and Technology, 2024).

5.4 NEN 7510

NEN 7510 is the information security standard within the Netherlands. It is based on the ISO/IEC 27001 and ISO/IEC 27002 norms (NEN, n.d.-a; NEN, n.d.-c). ISO/IEC 27002 is additional to ISO/IEC 27001, where ISO/IEC 27002 presents measures regarding information security. NEN 7510 is divided into two parts. The first part entails (the security of) management systems, where the second part offers measures to manage information security (NEN, n.d.-b).

5.4.1 Part 1: Management systems

Managing the CIA-triad of information is the general aim of information security. Within the healthcare sector, privacy of clients is dependent on managing the trustworthiness of personal health information. Next to this, the safety of health information of clients can mean the difference between life and death in certain situations. Therefore, the systems which store this kind of information have to be up all the time. Part 1 can also be seen as the Information Security Management System (ISMS) section of NEN 7510 (NEN, 2017).

Part 1 consists of two parts itself. The first part is created to foresee in requirements for determining, implementing, updating and continuously improving management systems which store client health information. Part 2 can be used by both internal and external instances to audit and judge the capabilities of organizations regarding the applicable information security requirements. For both parts 1 and 2 of the management systems part (part 1) of NEN 7510, there is no specific order in which implementations have to be done (NEN, 2020).

5.4.2 Part 2: Measures to manage information security

Part 2 (NEN 7510-2) is created to present guidelines for healthcare providers and other managing instances of personal healthcare information, regarding the CAI-triad. This second part of NEN is based on ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 277999. ISO/IEC 27799 offers healthcare specific needs in area of information security, as well as the unique working environment of the healthcare sector. The presented measures are based on ISO27002 (NEN, 2020). Each measure within NEN 7510-2 presents a target goal, which describes what the implementation or managing of the measure will mean for an organization. Then, the measure itself is presented, after which the healthcare specific measure and implementation guidelines are presented. Finally, healthcare specific implementation guidelines as well as any other additional information is presented, if applicable (NEN, 2017).

5.4.2.1 Plan, Do, Check, Act (PDCA) cycle

NEN 7510's ISMS is based on ISO/IEC 27001's ISMS. When NEN 7510 has to be implemented within healthcare organizations, it is mandatory that a working ISMS is in place. This way, audits for conforming to NEN 7510 can be performed. The ISMS is based on the Plan, Do, Check, Act (PDCA) cycle. Plan entails setting up the ISMS, Do entails implementing and executing the ISMS, Check entails monitoring and revising the ISMS, and Act entails the managing and improvement of the ISMS (NEN, 2017). There are different steps to be taken for each part of the PDCA cycle. These steps are presented in appendix 12.

5.5 De Nederlandsche Bank good practice on information security

The good practice Information Security by De Nederlandsche Bank (2023) presents 58 control measures to be on a high-level of information maturity. The good practice is specifically created for all organizations which are under control of DNB. The maturity model is based on the maturity model as presented in COBIT, which in turn used the CMMI maturity model. The good practice states that, at least for financial organizations, they are already on level three (defined). The healthcare sector is not in the scope of the good practice by DNB. But since all organizations which are under the control of DNB are banks, these controls could also be considered for the healthcare sector. This is because both sectors fall under the 'essential' category in NIS2, which means they have to implement the same measures (De Nederlandsche Bank, 2023).

5.5.1 Different types of controls within the Good Practice

The 58 controls presented in the good practice are based on several subjects. These subjects are governance, organization, people, processes, technology, facilities, outsourcing, testing, risk management cycle, and maturity model. This is presented below.

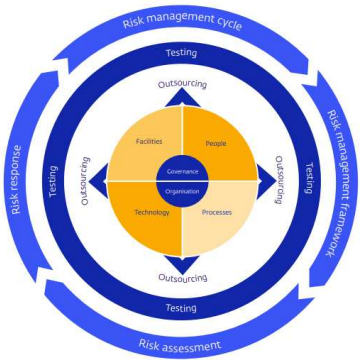


Figure 11: The subjects of the 58 controls in the Good Practice on Information Security (De Nederlandsche Bank, 2023).

Not all controls are evenly distributed among the subjects, since some subjects require more or less attention regarding information security. Organizations may choose to check the impact of outsourcing for each individual measure. This way, measures for managing risks can be taken into account in determining the level of maturity of an organization (De Nederlandsche Bank, 2023). This is also important for the supply chain cybersecurity which is highlighted in NIS2.

5.5.2 Maturity

The good practice offers a maturity model, which can be determined based on a self-assessment by an organization. This maturity model is based on the maturity model presented by COBIT. The model presents five levels of maturity which an organization can be at, or on level '0' if no attention is spend on a specific control. The level of maturity has to be determined for each of the 58 controls. The levels are (translated) 1) initial; 2) repeated but informal; 3) defined; 4) effective and measurable based on control measures; and 5) continuously improving and control measures are future focused (De Nederlandsche Bank, 2023). Appendix 26 presents the maturity levels in detail.

6 NIS2 framework

In this chapter, the NIS2 framework will be presented. Based on the differences (gaps) found between NEN 7510 and NIS2, and the specific frameworks presented in chapter 5, the framework is formed. Based on the literature review, an advisory report setup would be the most logical form in which the NIS2 framework can be created and used. By not only determining which elements a healthcare organization lacks but also by advising which steps to be taken next, the framework becomes the most useful. This way, organizations within the healthcare sector will be able to comply with NIS2.

By having three iterations of the framework, as presented in chapters 1 and 4, the framework is built. The first iteration is built upon the NIS2 in context chapter and the literature review, where the second and third iterations are based upon experts. This is done by both validating the framework as well as discussing with two experts based on internal documents how applicable the created framework is. The gaps (the elements which the healthcare sector doesn't have implemented yet) are presented in the framework. To find sufficient controls for these gaps, other frameworks are used. Not all frameworks cover NIS2, so different parts of other frameworks have to be used and combined. This is visualized in figure 12. For the specific control elements, advise is presented to prepare for and comply with NIS2.

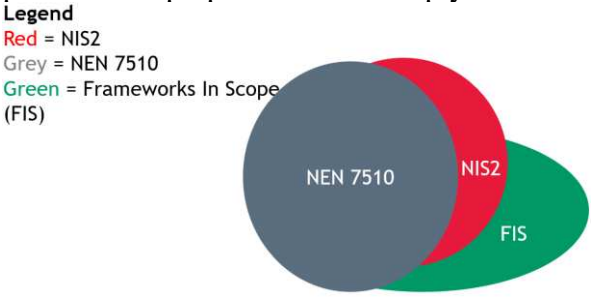


Figure 12: Comparison and overlapping parts of NIS2, NEN 7510 and other frameworks in scope of this research.

6.1 Gaps between NIS2 and the healthcare sector

By taking NEN 7510 as a starting point for the healthcare sector, there are quite a few mandatory requirements already implemented. This is not the case for everything, however. There are six gaps which still require specific things to be set up or updated (based on the NIS2 in context chapter, literature review and NIS2 framework comparison presented in appendix 13). These are 1) incident management, 2) standardized reporting, 3) contact with the CSIRT, 4) standardized impact assessment, 5) mandatory cybersecurity risk education for management, and 6) supply chain cybersecurity assessment. Appendix 27 presents how controls for the gaps have been created based on frameworks which were in scope of the research. Based on the overview of gaps presented

in appendix 13, the result of the analysis with specific controls is presented in the following paragraphs.

6.2 Framework

This paragraph presents the framework with the associated topics and controls for the identified gaps, as presented in the previous paragraph. The presented framework shows all the necessary controls for each identified gap. Since not every healthcare organization has the same IT personnel and resources, it may not be doable to implement all controls. This has also been commented by every interviewee to verify the initially created framework. Therefore, the most important controls to be fulfilled for each gap are worked out in the next paragraph. In the following table, all controls for the gaps are presented. This is the ideal situation, where all healthcare organizations should head towards. The paragraphs after the full framework present different maturity levels to distinguish between the bare minimum needed set of controls and the ideal, final situation regarding NIS2 in the Dutch healthcare sector.

In general, the role 'security officer' has been used to assign most controls to specific personnel. This role is however very broad, and can be swapped with a similar role within healthcare organizations. The different iterations of the framework have been presented by using color coding. The first iteration of the framework does not have any color coding. The second iteration of the framework presents changes to mostly controls, as well as a few extra topics. Changes regarding the second iteration are presented in blue. Changes in the third iteration are presented in green. When both after iteration 2 and iteration 3 changes were made, both colors are presented.

Gap (G)	Explanation	Topic	Control	Maturity level
G1: Incident management	A standardized incident reporting procedure needs to be created. Incidents need to be assessed so that these can be reported sufficiently to the CSIRT.	G1T1: Set up a standardized incident report.	G1T1C1: The security officer (or someone who is responsible for that role) creates a standardized report based on the Wbni reporting standard (see appendix 14).	2
		G1T2: Monitor potential threats.	G1T2C1: Current and future threats are identified based on incident logs and evaluated on a monthly basis by the security officer.	2
			G1T2C2: Logging of incidents is done in a SIEM (Security Information and Event Management) solution. This is evaluated on a daily basis by the security officer.	3
			G1T2C3: The security officer sets up a Security Operations Center (SOC) or Cyber Defense	3

Gap (G)	Explanation	Topic	Control	Maturity level
			Center, or alternatively, the organization makes use of a commercial external SOC. The input of the SOC or Cyber Defense Center is checked and evaluated monthly.	
		G1T3: Update the IT incident framework on a yearly basis.	G1T3C1: The security officer evaluates and updates the IT incident management framework/incident response plan on a yearly basis. This is done based on lessons learned from incidents which occurred either within the organization itself (incident logs), or by looking at incidents which occurred within similar organizations. This includes splitting privacy and cybersecurity risks.	2
		G1T4: Set up an incident response team.	G1T4C1: The security officer creates an incident response team which consists of the security officer, a senior IT manager, and a doctor which is part of the crisis team. After a significant incident, the composition of the team is evaluated and updated if necessary.	2
		G1T5: Audit/test the current IT incident framework on a yearly basis.	G1T5C1: The security officer creates and sets up a small awareness campaign for operational personnel each month. Once a year, a big awareness campaign is created.	2
			G1T5C2: An external, independent auditor audits the current IT incident framework on a yearly basis. The security officer is responsible for contacting the correct organizations/people for this.	4
		G1T6: Incidents are tested and simulated frequently.	G1T6C1: The security officer sets up penetration tests (pentests) to test the security in the network based on a risk analysis.	2
			G1T6C2: The security officer, together with the incident management team, simulates different cyberincidents on an annual basis among different departments on an annual basis.	2

Gap (G)	Explanation	Topic	Control	Maturity level
G2: Standardized reporting	A standardized way of reporting incidents needs to be created, so that each incident report is the same in setup.	G2T1: Communicate important (parts of) details to stakeholders, based on SLA's and agreements.	G2T1C1: The security officer updates the risk profile after a significant incident[10] has occurred.	2
			G2T1C2: The security officer, together with management, determines what information is communicated to stakeholders after an incident has occurred.	2
		G2T2: Report the different incident reports based on the timeframe after which an incident has occurred.	G2T2C1: The security officer creates and reports an incident reporting report to the CSIRT within the first 24 hours of a significant incident occurred based on the obligatory reporting tasks and process (see appendix 16).	2
			G2T2C2: The security officer, together with the incident response team, creates and reports an incident reporting report to the CSIRT within the first 72 hours of a significant incident occurred based on the obligatory reporting tasks and process (see appendix 16).	2
			G2T2C3: The security officer, together with the incident response team, creates and reports an incident reporting report to the CSIRT within a month of a significant incident occurred based on the obligatory reporting tasks and process (see appendix 16).	2
			G2T2C4: The security officer, together with the incident response team, creates and reports an incident reporting report to the CSIRT if the CSIRT requests an intermediary report based on the obligatory reporting tasks and process (see appendix 16).	2

[10] An incident is considered significant when it leads to operational disruption within the organisation, financial losses within the organization or to disruptions for others by causing considerable material or immaterial damage (Digital Trust Center, 2023; Overheid.nl; 2024).

Gap (G)	Explanation	Topic	Control	Maturity level
G3: Contact with the CSIRT	A lot of communication and information will come from, with or via the CSIRTs. Getting in contact with the relevant CSIRTs should be done as soon as possible.	G3T1: Events and information sessions from relevant CSIRTs need to be attended.	G3T1C1: The security officer and the incident response team attends (online or physical) seminars or events from Z-CERT NCSC and (national CSIRT) once per year.	2
		G3T2: The relevant CSIRT needs to be contacted.	G3T2C1: The security officer evaluates with both Z-CERT and the NCSC if all contact details are still correct each year.	2
G4: Standardized impact assessment	Reporting incidents can only be done if a sufficient impact assessment has been conducted. A standardized method for assessing the impact of an incident needs to be created.	G4T1: Set up a method to assess the potential impact of incidents.	G4T1C1: The security officer does the first impact assessment of occurred incidents. If applicable, this is done together with the finder(s) of the incident.	2
			G4T1C2: The incident response team assesses the impact of a significant incident. Based on the outcome, the necessary information needs to be collected as well as people to help with the reporting process. For the incident assessment process, see appendix 16.	2
			G4T1C3: The incident response team identifies, evaluates, prioritizes and processes solutions to occurred incidents. This needs to be based on the impact and urgency of the change.	2
		G4T2: Collect and document the potential impact of the incident so that it can be reported.	G4T2C1: The incident response team, together with the security officer and other identified employees related to the incident, classify and prioritize incidents based on pre-determined criteria. A Root Cause Analysis (RCA) is conducted. The incidents with the highest priority are handled first.	2
G5: Mandatory cybersecurity risk education for management	Management needs to develop competencies to assess be able to identify the risks regarding the security of	G5T1: The policy regarding management training and awareness is created or updated.	G5T1C1: The trainings plan regarding risk education is updated by the security officer, which includes mandatory trainings, exercises or tests for management. Updates to this plan occur on an annual basis.	2

Gap (G)	Explanation	Topic	Control	Maturity level
	network- and information systems, to judge the current risk control measures, and to judge implications of risks and risk control measures. This needs to be based on participation in tests and exercises.	G5T2: Training requirements for management need to be defined.	G5T2C1: Management's level of knowledge/skills regarding cybersecurity risk education is assessed at least every 3 years. The security officer places this in the policy regarding risk education.	2
			G5T2C2: The security officer, together with the human resources department, defines the required knowledge and skill levels mandatory for management. Trainings, tests and exercises are presented in a policy. This policy is updated every 3 years.	2
		G5T3: Trainings, tests and exercises need to be regularly conducted.	G5T3C1: The security officer sets up at least one training/exercise/test per year for management. This may also be outsourced to instances with more experience regarding cybersecurity risk education for management specifically.	2
			G5T3C2: The security officer sets up at least one training/exercise/test semi-annually for management. This may also be outsourced to instances with more experience regarding cybersecurity risk education for management specifically.	3
		G5T4: Management needs to be able to prove that they own the necessary skills and competencies.	G5T4C1: The security officer sets up certificates of completion, mandatory attendance (lists) and tests in the policy regarding risk education which management members can use to prove their competency levels.	2
G6: Supply chain cybersecurity assessment	The entire supply chain of information sending and receiving with external organizations needs to be assessed to improve	G6T1: A list of all external organizations which either sends or receives information of the organization needs to be documented.	G6T1C1: The procurement manager creates or retrieves a list of al external partner organizations. This list is updated on an annual basis.	2
			G6T1C2: The procurement manager, together with the security officer, identifies all external partner organizations which are in the strategic quadrant ('strategisch', high supply risk and high impact risk if this partner cannot deliver information/their services) based on appendix 15.	2

Gap (G)	Explanation	Topic	Control	Maturity level
	cybersecurity in the entire supply chain.		G6T1C3: The procurement manager, together with the security officer, identifies all external partner organizations which are in the lever and bottleneck quadrants (‘Hefboom’: low supply risk and high impact risk and ‘knelpunt’: high supply risk and low impact if this partner cannot deliver information/their services) based on appendix 15.	3
			G6T1C4: The procurement manager, together with the security officer, identifies all external partner organizations which are in the routine quadrant (‘Routine’: low supply risk and low impact risk if this partner cannot deliver information/their services) based on appendix 15.	4
		G6T2: A minimum level of cybersecurity measures is determined which will become required to continue to collaborate with the organization.	G6T2C1: For the identified external partner organizations, the security officer defines a minimum level of maturity see appendix 15). This list is evaluated yearly by the procurement manager and the security manager.	2
			G6T2C2: For each subset of cybersecurity controls, the required maturity level for different types of external partner organizations are defined by the procurement manager as well as the security officer. This can also be defined in terms of certifications, such as the NIS2 quality mark. The important/important (strategic) quadrant always needs to present an assurance report. The required maturity levels are evaluated and updated if necessary on an annual basis.	2
		G6T3: Each external organization needs to be mapped and prioritized based on the potential risk of information not	G6T3C1: The procurement manager contacts the people in charge of partner management of external partner organizations, to schedule a meeting to identify the current cybersecurity (subsets of) controls. This process is repeated on an annual basis.	2
			G6T3C2: Based on the minimum cybersecurity measures (different subsets of controls) implemented at the external partner organizations, a maturity level is assigned to each	2

Gap (G)	Explanation	Topic	Control	Maturity level
		being delivered or received.	subset of current controls by the procurement manager and security officer. This is done in collaboration with the external partner organization and evaluated and updated if necessary on an annual basis.	
			G6T3C3: Each identified maturity level which is below the required/defined threshold needs to be documented for each external partner organization by the procurement manager and security officer. Each month the procurement manager checks if any changes have occurred and updates the list if necessary.	2
		G6T4: For each identified/known external organization, the current SLA's and contracts are updated with the new minimum cybersecurity measures.	G6T4C1: For each identified gap, a set of measures to implement has to be presented to the external partner organization by the procurement manager and management in the form of an updated SLA or contract. This process is repeated, if necessary, on an annual basis.	2
			G6T4C2: The partner procurement manager of external partner organizations presents metrics or a dashboard or a report of the new requirements so that management can assess the current supply chain cybersecurity measures efficiently. This update is based on agreed service level reporting or similar standards in the service level agreement.	2
		G6T5: Minimum cybersecurity requirements are presented in SLA's of future partner organizations.	G6T5C1: The standard contract/SLA for collaborations with new partner organizations is updated with the new mandatory cybersecurity standards by the procurement manager together with the security officer.	2
			G6T5C2: The IT department/the security officer is involved in the process of acquiring new partnerships. The procurement manager needs permission for a partnership from the IT department/the security officer if the cybersecurity requirements are present at the potential new partner organization.	2

Gap (G)	Explanation	Topic	Control	Maturity level
		G6T6: Decisions regarding the continuity of partnerships with external organizations need to be made.	G6T6C1: After one year between the procurement manager and the external partner organizations' procurement manager and/or management, the implemented required measures to continue the partnership between the two organizations is assessed by either the procurement manager and/or the security officer or by an external auditor.	2
			G6T6C2: Based on the outcome of the assessment of measures, a decision is made by management to continue the partnership or to terminate the contract. This is done each time the outcome of an assessment is not sufficient for the continuation of a partnership.	2
			G6T6C3: For any soon to be terminated contract, a new supplier needs to be found by the procurement manager which does have the required cybersecurity (subsets of) controls in place. This is done each time the outcome of an assessment is not sufficient for the continuation of the partnership.	2

6.2.1 Controls in detail: maturity levels

To assure compliance with NIS2 regarding the gaps, it has been chosen to work with maturity levels, as presented in the good practice on information security by DNB (see paragraph 5.5.2).

There are 5 maturity levels. The lowest level (level 1) would be complying with NEN 7510. However, the verification interviews (experts 2, 4 and 6) showed that this is not always the case, despite NEN 7510 being mandatory for healthcare organizations. This means that organizations can also be on level 0, which would indicate that NEN 7510 has not been implemented fully yet. Level 2 would indicate a minimum level in order to comply with NIS2 (the Cbw). A difference is made between hospitals and all other healthcare organizations. Level 3 would indicate a more sufficient level, where hospitals have to comply with. Level 4 would indicate the complete set of controls to be implemented, where level 5 would indicate that all controls are proactively managed and that improvements are made each year.

6.2.1.1 Maturity level 0: Ad Hoc/ on the way to NEN 7510

This maturity level is assigned to healthcare organizations if they are not fully compliant with NEN 7510. Experts 2, 4, and 6 mentioned that healthcare organizations often times want to execute their processes based on NEN 7510, but not own a certification for it. This means that in practice, healthcare organizations are not ready for NIS2 yet, where they should be, since NEN 7510 has been mandatory for healthcare organizations since 2016 according to expert 6.

6.2.1.2 Maturity level 1: NEN 7510

Healthcare organizations which are NEN 7510 certified are maturity level 1 regarding NIS2. This level is the starting point to work towards NIS2, since the identified gaps have been based on this as well as the fact that NEN 7510 has been obligatory since 2016 according to expert 6. As presented in the literature review, it was expected that seventy out of seventy-seven hospitals in the Netherlands have implemented NEN 7510 in 2023 (Inspectie Gezondheidszorg en Jeugd, 2023).

6.2.1.3 Maturity level 2: The minimum level

Maturity level two ensures that the bare minimum in order to comply with NIS2 is implemented. This level is sufficient for all healthcare organizations except hospitals. The bare minimum includes at least one or more controls from all six identified gaps.

6.2.1.4 Maturity level 3: Mandatory for hospitals

Since hospitals simply have a higher risk of very severe direct consequences regarding cybersecurity incidents, it is therefore necessary that they implement more controls to manage more risks regarding cybersecurity than all other healthcare organizations. The supply chain needs to be evaluated more clearly, and in general all employees need to be more aware and trained to deal with incidents. This also applies to management.

6.2.1.5 Maturity level 4: The complete set of controls

The full set of controls is the ideal situation to work towards. This set of controls is subject to change in the form of minor additions or changes. This is because the final version of the Cbw may still change based on the internet consultation where feedback is presented.

6.2.1.6 Maturity level 5: The complete set of controls proactively managed and improved

As the good practice on information security by DNB stated, the final maturity level is based on a continuous improvement and evaluation cycle of the current controls in place. This includes the control measures being updated continuously, where evaluations are based on the future. Peer-based benchmarks are taken into account with evaluating the controls. The controls are benchmarked based on external data, the effectiveness of the controls is measures based on KPI's and employees are proactively involved (at all times) in improving the controls (De Nederlandsche Bank, 2023). These steps all have to be done for the complete list of controls presented in the framework to reach maturity level 5.

6.3 Elaborations on framework iterations

The framework has been updated through three iterations, as presented in chapter 4.1. Based on the different interviews, a general remark was that the framework looks to be very complete, but too much to implement for smaller healthcare organizations. Expert 10 stated this specifically: "*A hospital is significantly different than a small GP or disabled people organization. Frequencies for controls will be once per year a lot of the times for smaller organizations, but for bigger organizations where there are a lot more risks, you would want the frequency of certain controls to be much higher than once per year*". This resulted in the development of maturity levels for different controls. The final framework also presents different maturity levels, as presented in the previous paragraph. For BDO, an Excel-version of the framework has been created, where the maturity levels can be individually selected for the corresponding maturity level. Appendix 25 presents a snippet of the Excel-framework.

6.3.1 Iteration 1

The first iteration of the framework is based on the NIS2 in context chapter (H2), the literature review (H3), and the current framework analysis (H5).

6.3.2 Iteration 2

The second iteration of the framework is based on 10 expert interviews. As presented in appendix 22, each conducted interview was done with either a cybersecurity expert, a healthcare expert or someone who is an expert in both groups. The changes in the framework based on the interviews have been color coded in blue. Deleted controls have either been reformatted into another control, or fused with another already existing

control. This is because some controls were similar to each other or not necessary since it was already covered in another control. For each changed control, an elaboration is given as well as quotes from the interviews with the experts.

6.3.2.1 Changes in gap 1

G1T2C1 & G1T2C2: these controls were originally only one control. The control was too big, and a SIEM is too big to implement for smaller healthcare organizations. This meant a SIEM is more realistic for maturity level 3 than 2. Expert 10: "*I think that a SIEM solution is already a pretty high maturity level*". Expert 4: "*I don't think that the average healthcare organization is very proactive in monitoring threats. (...) incident logs which are evaluated can also work*". Expert 7: "*Smaller healthcare organizations, I think, don't have a SIEM. Hospitals are however working with this. Sometimes smaller organizations have other solutions. A SIEM for a smaller organization is less realistic*"

G1T3C1: this control has been updated, since updating the incident response plan needed to emphasize learning for previous events (reflecting) on incidents more. Next to this, there are often incident response plans in place, but they often do not distinguish between cybersecurity and privacy risks/incidents.

Expert 7: "*An example of a hospital where I have been privacy and security (risks/incidents) were always handled together. Now you see a shift towards splitting this*". Expert 10: "I*t would be nice to take an incident which has occurred at a neighbor organization*"

G1T5C1: the importance of awareness campaigns had to be emphasized more clearly in the framework. And awareness campaigns are not part of a business continuity plan (BCP), which is also changed. Expert 7: "*An awareness campaign is part of a policy*". Expert 1: "*Since awareness is important, healthcare organizations have bought e-learnings for their employees. Then you see that in practice only 1 hour is spend on these. And then this is the project which they have been working on for two years, but they forget to think about the prioritization, what was the initial aim of the campaigns?"*. Expert 10: *"Awareness is something which is taken into account when a new person joins the organization, but I think that in general this can also improve on the content after this has occurred"*

G1T6, G1T6C1 and G1T6C2: Testing (in the form of penetration tests (pentests) and simulating incidents either does not happen or it happens not frequent enough to make a difference. Therefore, this topic and the controls were added to the framework. Expert 7: "*Simulating incidents does most of the time not happen at all. Having a policy regarding incident management is good, but if the incident management team has never seen it or met together to discuss the plan? No clue*". Expert 10: "*When I do cyber audits, I see that*

healthcare organizations could organize more frequent pentests, this is not done very often"

6.3.2.2 Changes in gap 2

G2T1C1 and G2T1C2: these controls have been created since the original control consisted of too many different parts. For example, updating the risk profile is now a separate control. Significant incidents specifically had to be mentioned in the updated controls. Finally, stakeholders do not need to be specified in the control. Expert 5: "*The healthcare professional cannot decide on its own what incident is priority 1. So I'm really hesitant to say that regular incident management is their task*". Expert 8: "*Splitting the risk profile to another control is easier*"

6.3.2.3 Changes in gap 3

G3T1C1, G3T1C2 and G3T1C3: these controls were only one control in the first iteration which looked like G3T1C3. The interviews showed that more had to be done with the CSIRTs than just managing the contact with them for reporting purposes. Z-CERT periodically offers (online) seminars or events where healthcare organizations can ask questions and be informed about the latest information, news, and tips. People which have to deal/collaborate with Z-SIRT and CSIRTs in general (such as the security officer and the IT Incident team) should attend these sessions. Expert 4: "*I attended a session of the NCSC (the national CSIRT) which will become the central reporting organization for incidents. This would mean that you don't need to have contact with branch specific CSIRTs. (...) If you are a healthcare provider, information regarding incidents which occur in one sector come from Z-CERT*". Expert 3: "*The NCSC is currently working on creating a central reporting location for incident reporting. (...) NCSC asks Z-CERT to update healthcare organizations with relevant information regarding incidents which may apply to all or a lot healthcare organizations, such as with a ransomware attack*". Expert 7: "*You could create a control where there is a periodical consultation regarding cybersecurity healthcare sector subjects. If there is nothing to be discussed, this consultation can be very brief. (...) I believe that Z-CERT has periodical gatherings where you can register yourself for. Someone important from the healthcare organization could join these gatherings*". Expert 1: "*I think that for healthcare organizations, you should determine who is responsible for reporting and to who. How is this organized in practice?*"

6.3.2.4 Changes in gap 4

G4T1C1: this control has been changed slightly since the ways how good controls are setup should be based on the 5 W's and the 1 H. In almost every interview this was mentioned for creating good controls. The 5 W's consist of the who, what, where, why, when and the H for the how. Expert 2: "*It starts with the 5 W's and the How. That is the standard for formulating controls. (...) I think the most frequently made mistake is that people create control activities instead of an actual control description*"

G4T2C1: Conducting a RCA should be done, but this is too much to list together with determining solutions or workarounds to occurred incidents. Next to this, only one person should be responsible for the RCA. Finally, incidents with the highest priority are handled first. This was originally not part of the control. Expert 5: "*Healthcare organizations should determine what us a critical incident, and within how many days does it need to be solved? What is the procedure for this?*".

6.3.2.5 Changes in gap 5

G5T2 and G5T1C1: these controls have been changed so that the Business Continuity Plan (BCP) is no longer part of the control. In practice, the BCP is not used for management training protocols, this is often presented in another policy of the organization. Finally, this policy is not executed or set up by management, which was originally the case. Expert 2: "*Security incidents are a lot bigger than just a backup and restore, so I think that the scope of the document should be broader*". Expert 4: "*Your control "management creates and updates the BCP" is too specialized, management for sure does not know how to formulate a BCP*". Expert 5: "*The part of a BCP I wouldn't make part of this gap and set of controls. (...) The training should be there, but I wouldn't specifically mention it in a BCP*".

G5T2C1: The frequency of assessing the skills of management usually happens every 3 years in practice. This is because the baseline of management should be assessable. If new updates to the skill levels are presented in training policies, there is no baseline to test if management actually broadened their skill levels. Expert 10: "*Maybe you should assess the skills of management every 3 years, since this would make the skill levels measurable. You want to prevent that you cannot measure the skill levels if you keep on changing the baseline skill levels of management*".

G5T3C1, G5T3C2 and G5T4C1: There are two versions of the same control but with different frequencies presented, which are there for maturity levels 2 (annually) and 3 (semi-annually). Next to this, certifications, tests and attendance lists can work in practice to measure the training and skill level obligation of NIS2. Finally, trainings for management have to be split up and be set up in a different manner than for operational

healthcare personnel. This is because management is not working on operational levels, and therefore has different needs for training and education. Expert 8: "*No one will be updating the management education plan every month. If this happens twice a year, it is already a lot. But updates to policies happen in general once per year*". Expert 6: "*The employees only need to know what they need for their day-to-day activities. I think it is also beneficial that they do not know what management's tasks are*" Expert 9: "*I think that mandatory attendance is always very important, to be able to audit if policies are actually executed the way they are intended to. (...) I'm a fan of certificates. In the end, it is the easiest way to check if someone has gathered the sufficient knowledge levels in order to continue*".

6.3.2.6 Changes in gap 6

G6T1C2, G6T1C3, G6T1C4, G6T2C1 and G6T2C2: these controls are based on maturity levels. For different maturity levels, increasingly more external partners should be assessed regarding their supply chain risks and management. This applies to G6T1C2, G6T1C3 & G6T1C4, which are for maturity levels 2, 3 and 4. The controls G6T2C1 and G6T2C2 apply to the identified external partners regarding their cybersecurity levels and the minimum required threshold in order to continue the partnership with the healthcare organization. Expert 1: "*I have worked for an organization which took a very technical approach to applying cybersecurity prevention measures. They wanted to install MFA from Microsoft, but they didn't take the managing board with their thinking process. The managing board did not want their employees to use their own mobile phone in the working environment. In the end, they said they implemented 'everything' except MFA, because the managing board did not allow it*". Expert 6: "*You see in practice that maturity models such as CMMI are used for controls. Level 3 out of 5 is than working according to a certain procedure and you can prove that you have done the procedure. (...) With these principles in thought, you could create a classification model where you plot all the controls/measures in*". Expert 8: "*Maturity levels of the controls in the supply chain are required from suppliers. You could say that an organization which uses an EPD where the risk is higher, requires more controls than for an organization which offers a much lower risk-impact application*". Expert 7: "*I think that it is logical that hospitals are a target faster than smaller healthcare organizations, so it makes sense that they are a higher maturity level*". Expert 9: "*You could even make a graphic related to the maturity levels, where you look at where to we have an elevated cybersecurity risk? This is definitely the hospitals, they are really in an elevated cybersecurity risk. A smaller GGZ instance that maybe owns two buildings where 200 patients are, is then a substantially smaller target. (...) The rules that apply to hospitals are less realistic for smaller organizations*". Expert 10: "*The healthcare sector is very broad, and the frequences of*

executing the controls is just different in a hospital than in a smaller disability organization. (…) You will probably end up with at least once a year for a lot of controls, where you would want the frequency to be much higher for bigger organizations where there are a lot more risks".

G6T3C1 & G6T3C2: These controls have only changed in frequency. Updates to policies generally occur once per year. Expert 8: "*Updates to policies happen in general once per year*". Expert 5: "*You would want to have a policy be created where the policy itself is evaluated on a yearly basis, where updates can occur if the current policy has become insufficient*".

G6T4C1 & G6T4C2: These controls have changed in frequency, since updates to policies only happens once per year (see the elaboration for the controls G6T3C1 and G6T3C2 above). Next to this, having to present the current level of implemented measures is often presented via service level reporting, which comes from the SLA. Expert 2: *Contracts are defined with SLAs. Often times, good conversations happen, but afterwards checking if the partner organization is performing conform the SLA via service level reporting or asking for an assurance statement is not done often. Sometimes, the partner organization is proactive and sends them anyway, but often times no real assessment is done*". Expert 3: "*In practice, you see that in an operational level service level agreements and service level reporting takes place. (…) But elements related to cybersecurity are very rarely mentioned in these reports and agreements*". Expert 10: "*Supplier management could definitely be improved*".

G6T5C1 & G6T5C2: The procurement manager should be responsible for contract management together with the security officer for updating the contracts with the new required cybersecurity elements in SLA's for example. When new potential partners are found, the IT department (for example, the security officer) needs to decide if the presented cybersecurity controls are actually in place. IT was not taken into the procurement process with new software suppliers previously, which is important if the baseline cybersecurity levels have to be reached and kept the same for all types of partner organizations. Expert: 5: "*The procurement department could use a list where the type of organization is listed. When a potential new partner organization is category 2 for example, we require (as a healthcare organization) the following requirements. The final risk calculation or analysis could be done by an IT manager. (…) The IT manager owns the technical skills*". Expert 2: "*You could create a preventative control which states that for finalizing new partner contracts the process of cybersecurity assessment based on the cybersecurity requirements for suppliers is checked before accepting a partnership*".

G6T6C1: It is important that changes to cybersecurity controls/measures are checked over time, to assess if the situation of a partner organization has improved based on the suggested improvements by the healthcare organization. This was previously not part of

this control. Expert 9: "*The software could be improved just enough by suppliers so that compliance is reached. An example that I have seen is that at the start a measurement for the baseline level is done, after which an improvement plan is presented. Then within 2 or 3 years, improvements happen and compliance is met. But if the system is not continuously improved, the change stagnates over time*".

6.3.3 Iteration 3

The third iteration of the framework is based on 2 validation interviews with experts by using the IT audit protocol called 'cyber in the audit'. This protocol tests for a specific organization (in this case a healthcare organization) the controls. By comparing the controls presented in the framework with the controls and measures used in the healthcare field, details such as the frequency could be updated. As presented in appendix 22, the two experts are both experts in the healthcare field and known with auditing healthcare organizations. Both maturity levels 2 and 3 were tested by picking (and anonymizing) a healthcare organization which is not a hospital (maturity level 2), and a hospital (maturity level 3). The changes in the framework based on the interviews have been color coded in green. Quotes and elaborations are presented to explain the changes to the controls. The frequencies of the controls which are sufficient are not updated, since the validation interviews concluded that they were corresponding to the real-life scenarios based on the cyber in the audit check for hospitals and non-hospital healthcare organizations.

6.3.3.1 Changes in gap 1

G1T2C1: Monitoring on a daily basis is changed to a monthly basis. Expert 11: "*This could be done on a monthly basis*".

G1T4C1: Each three months evaluating the team composition was too much. This needs to be done on an ad-hoc basis. Next to this, the financial controller should not be part of the incident response team, but rather a doctor. This has also been changed. Expert 9: "*The first thing that I would think of is the involving the responsible person of the doctors. If everything stops working, it may be the case that financial reporting needs to have a say in it as well. But that is not the priority. The priority is that the patients are not impacted*". Expert 11: "*I don't think that evaluating the composition of the team needs to be done each three months, but rather on an ad hoc basis after an incident has occurred*".

G1T5C1: An awareness campaign each month is doable, but only if these are very small in size, such as a phishing email one month and a poster regarding cybersecurity awareness on toilets for example in another month. A big awareness campaign needs to be done on a yearly basis. Expert 9: "*An awareness campaign is something which needs to occur on a continuous basis rather than ad hoc once a year (…) Awareness campaigns*

can already be as small as placing a poster in the bathroom or sending an email". Expert 11: "*I don't think that security awareness campaigns on a monthly basis is realistic*"

G1T6C1: A pentest is done on the network, and not on a specific application which was what the control stated in iteration 2 of the framework. The frequency has been deleted, since this is determined based on the risk analysis per application. Expert 9: "*A risk analysis needs to be done, and bass on this outcome the frequency is determined*". Expert 11: "*A pentest is not done on an application, but on a network*".

G1T6C2: Simulation of cybersecurity incidents should be done on a yearly basis rather than on a semiannual basis. Expert 9: "*Once or twice per year this hospital has dedicated crisis moments simulated*". Expert 11: "*This is almost always done on a yearly basis*".

6.3.3.2 Changes in gap 2

G2T1C1, G2T1C2, G2T1C3: In iteration 2 there was a control which stated that the security officer tests the incident procedure on a yearly basis. This entire control has been deleted, since the incident procedure is already tested when an incident has occurred. This meant that G2T1C2 and G2T1C3 have now become G2T1C1 and G2T1C2 respectively. Expert 9: "*I agree to remove this control*". Expert 11: "*The incident procedure is not tested, since this is already done when incidents occur*".

G2T1C2: The word 'significant' has been removed, since communication to stakeholders always needs to be done and determined what to share, despite the size of the incident. Expert 11: "*For privacy incidents for example that may not lead to a disruption, stakeholders also have to be informed*".

6.3.3.3 Changes in gap 3

G3T1C1: Originally, attending events or seminars from both the NCSC and Z-CERT were separate controls. These have been merged. Next to this, the frequency has been updated to attending the events once per year. Expert 9: "*Such an event is often times an entire day, and then you lose an important employee for that day. I would rather say that they would be obliged to attend such a training once per year (...) I don't see any value in keeping the controls of the Z-CERT and NCSC apart*". Expert 11: "*This customer is very good in attending such events*".

G3T2C1: Checking/updating contact details only needs to be done on a yearly basis, and not on a monthly basis which was originally the case. Expert 9: "*I would rather say that this is done on a yearly basis*". Expert 11: "*I think that on a monthly basis is too much. It should be yearly*".

6.3.3.4 Changes in gap 4

G4T1C3: Identification, evaluation, prioritization and processing of solutions is not done via change management. This has been deleted from the control. Expert 9: "*This is a separate process than change management*". Expert 11: "*It is not per se done via change management*".

G4T2C1: Originally, there was a separate control which stated that solutions for incidents were identified. This control has been deleted since it was already part of control G4T1C3. Expert 9: "*I would combine these controls and have the root cause analysis in another control*".

6.3.3.5 Changes in gap 5

G5T1C1: Information regarding education for employees is presented in a trainings plan, and not in a policy, which was originally presented in iteration 2 of the framework. Expert 9: "*I don't really see this in practice*". Expert 11: "*It is not really a procedure, but rather a trainings plan*".

6.3.3.6 Changes in gap 6

G6T1C1: Updating the list of partner organizations is done on a yearly basis instead of twice a year which was originally presented in the control. Expert 9: "*In general, updates happen once a year*". Expert 11: "*In practice I noticed that such a list is only made in a limited fashion*".

G6T2C2: The most critical applications/software which are used (the ones identified as strategic in the Kraljic matrix) always need to present assurance reports. This is added to the control. Expert 9: "*You have to consider what application you are working with*". Expert 11: "*A yearly report is inevitably mandatory (...) For us as an external party, a conversation is not enough. You would need an assurance report, which is issued on a yearly basis (...) This healthcare organization does not demand cybersecurity controls from their partner organization, but this is critical of course*".

G6T4C1: The control originally mentioned that workarounds need to be in place at the external partner organization. In practice, this is always already presented, so this information has been removed from the control due to redundance. Expert 9: "*In general this is already in place in the initial contract*".

G6T4C2: Not all organizations have service level reporting. Therefore, the control has been expanded with 'or a similar reporting form'. Expert 11: "*Not all customers have service level reporting*".

G6T5C2: In practice, it may be very hard to involve the IT department in small healthcare organizations in the process of acquiring a new application or software. This

is because small healthcare organizations may only have one person in charge of IT, which has several tasks and roles to do. Therefore, the control has been changed so that this person which represents the IT department, if there is none or if it is outsourced, is still involved but does not make the final decision to acquire the new application or software. Expert 9: "*Sometimes you have a procurement manager which is also the HR manager and is also in charge of supply chain management (…) You cannot make a choice about IT without your IT department, since they are in charge of implementing the system or application*". Expert 11: "*The IT Department or security officer is not often involved in the acquiring process of a new application or software (…) In 9 out of 10 healthcare organizations this is not the case. For hospitals this could be the case more often, but not for smaller healthcare organizations*".

G6T6C1: Assessing if the measures to improve the cybersecurity standards have improved at external partner organizations occur once per year. Originally, the control stated that this happened after 'an agreed period of time'. Expert 9: "*I would say this is done yearly*". Expert 11: "*This healthcare organization evaluates periodically if the application still fits their needs based on a cycle of 4-years. Not every application is evaluated at the same time, but one application one year, and another application in a different year*".

7 Discussion & results

This chapter contains the discussion section, and it discusses the results from the research as well as the contributions to theory and practice. Finally, the limitations & recommendations for future research are presented.

7.1 Discussion

The pilot interviews showed that just asking questions and then continuing to ask more pre-determined questions does not work in practice while talking about specific controls and known frameworks. Therefore, a semi-structured interview setup was preferred for the verification and validation interviews. Next to this, a small survey was conducted prior to the pilot interviews. The idea was that based on the outcomes of the survey, follow-up questions could be determined. This turned out to not be practical at all; the verification and validation interviews would not be similar among interviewees and analyzing the results would not result in data saturation. Therefore, the choice to not use surveys in the research was also made.

By having 10 different interviews with experts within both the cybersecurity and healthcare sector which ended up responding in a similar fashion, it meant that the desired data saturation as presented in chapter 4 (methodology) was reached. An example of this is the similar answer on the question “how can you create a sufficient control?”. 8/10 interviewees answered that in order to create a sufficient control the with the 5 W’s and the How (Who, What, Where, When, Why, and How) needed to be kept in mind. Another example is the common answer on follow-up questions on the supply chain assessment. This turned out to be very difficult in practice. Several interviewees stated that pressuring vendors with a collective of healthcare organizations helps (and is possibly the only way) with making sure that changes to applications happen regarding NIS2 compliance. This is because healthcare organizations have major vendor lock-in problems regarding their application landscape. Several interviewees mentioned that there are only a few suppliers of healthcare systems, which causes this problem. This makes dealing with supply chain problems very difficult, especially if organizations are on their own.

The first iteration of the framework turned out to be too big. This resulted in a lot of responses from the experts that the controls are applicable in different levels only, and that one type of healthcare organization (with the specific mentioning of hospitals) needed to be distinguished. Some experts mentioned maturity levels to be implemented, such as the ones based on the CMMI. It should be noted that maturity was not in scope of the research, so it is only a first setup. Future research should include maturity models to improve the framework. The framework has been updated in between interviews, which also meant a first setup of maturity levels. In the interviews experts 7, 8, 9 and 10

have therefore briefly discussed the setup of maturity levels as a result of follow up questions. One of the main outcomes was that prioritization of the controls was important; determining which control is more important than another is one of the main improvement points. This also applied to the frequency of the controls; this could also vary between different types of healthcare organizations. Once again, it was mentioned that ideally you would want a higher frequency and more controls to be in place at hospitals due to the higher risk of falling victim to cybersecurity incidents.

Two technologies which are currently blooming are Artificial Intelligence (AI) and Internet of Things (IoT). These were also identified by Roodhooft (2024) in the literature review (paragraph 3.3). The identification of risks in the supply chain can be very hard, which a lot of experts mentioned. By using AI, it could be possible that in the future risks are mapped based on a risk profile and other variables such as the risk appetite of healthcare organizations and the amount of (sensible) data being transferred from supplier X to the healthcare organization and vice versa. Mapping and identifying cybersecurity risks in general could also happen with the help of AI in the future, which could decrease the administrative tasks for security officers.

Since the healthcare sector (specifically hospitals) uses a lot of IoT medical devices, there is a big risk in falling victim to cyberattacks if the interconnectivity (the network of connected IoT devices) is not sufficient. This network of IoT devices should be mapped (which could be done in the future with the help of AI) in order to assess where the most sensible information is being processed. Then, connections to suppliers or other healthcare organizations need to be identified. This information could once again be mapped automatically with the use of AI based on pre-defined variables. This could help with the identification of critical suppliers and systems in the network of the healthcare organization, which could flag these applications or suppliers. The flagged suppliers of applications can then automatically be labeled as a ‘high risk’ which would mean that they need to have more control measures in place. This could mean that a higher level of the NIS2 quality mark for example is required in order to continue the partnership with the supplier of an application.

7.2 Results

The pilot interviews conducted early on in the study suggested that the verification- and validation interviews needed to include more specific questions regarding the final framework. It showed that the approach on asking which parts were important for the creation of a NIS2 framework was too broad, and needed to be specified on controls coming from the actual framework. Next to this, the questions needed to be more concise and be elaborated on at times so that the interviewees would understand the reasoning behind certain questions.

The interviews with the ten experts showed that the framework was already pretty complete. In general, the feedback showed that the frequency of certain controls was not always correct. This has been validated and updated by using the IT audit method ‘cyber in the audit’. By looking at specific healthcare organizations, the frequency of the controls could be improved by looking both at real-life examples of cybersecurity measures combined with experts in the field.

The validation interviews only had a few minor deviations in terms of control setup feedback and frequency changes. In general, experts 9 and 11 agreed on the already presented frequencies coming from the verification interviews from iteration 2 of the framework. And when changes had to be made, they both mostly agreed (independent from each other) on the minor changes of controls and frequencies. Since not everything was agreed on, data saturation was not reached fully yet. Therefore, future research would have to look into more real-life examples (or case studies) into the practicality of the framework.

In general, the interviews quickly showed that the framework had to be redesigned to suit the real-life implementation better. Not all healthcare organizations are the same. A hospital may have several dozens of IT personnel, where a small local general practitioner may only have one IT person in charge of everything regarding IT. This meant that not every control could be implemented realistically. A logical solution for this was to divide the controls into maturity levels based on universally accepted standards. All experts in iteration 2 of the framework agreed that this was a logical step for the updated version of the framework. Next to this, bigger healthcare organizations are in general also bigger targets according to the experts. This meant that more controls are required for bigger organizations, such as hospitals. Not every organization is familiar with the term ‘maturity’, and therefore a generally accepted and well-known solution had to be used. The used maturity model setup was also approved in the validation interviews: experts 9 and 10 stated for example that this setup would work in the healthcare sector in general (expert 9: that is indeed a nice setup; expert 10: this setup sounds very logical).

It was also interesting that experts said that the healthcare sector is obliged to have NEN 7510 in place for almost 10 years now, but that in practice, ‘working conform NEN 7510’ is already enough to not get penalized with fines. This is also why healthcare organizations will most likely wait as long as possible with complying with NIS2, which has been stated several times by experts in the verification interviews.

7.3 Contribution to theory & practice

By providing a gap analysis between NIS2 and the healthcare sector in the Netherlands based on NEN 7510, healthcare organizations in the Netherlands are no longer unaware about the missing elements to comply with NIS2. By providing a list of controls, a practical implementation of a unique set of frameworks is presented. This has not been done before in academia, since NIS2 is not finalized yet at the time of writing. By providing the healthcare sector with specific controls to implement, they will be prepared to become NIS2 compliant to a maximum extent. By distinguishing between hospitals and other healthcare organizations based on verification and validation interviews with experts, practical limitations and real-life scenarios such as higher risks to be targeted for hospitals are taken into account.

7.4 Limitations & recommendations for future research

NEN 7510's parts 1 and 2 originate from 2017 and 2020 respectively. This means that it is somewhat outdated, despite having ISO/IEC 27001 and ISO/IEC 27002 implemented. This is because ISO/IEC 27001- and ISO/IEC 27002 have an updated version which originates from 2022. The updated versions have therefore not been placed into the scope of this research because of time constraints. Next to this, it is possible that the health sector will create their own cybersecurity controls or standard which healthcare organizations will have to comply with. Examples are a newer version of NEN 7510 or the XIS Quality Mark which is specifically for healthcare systems (XIS Keurmerk, 2024).

These quality marks could offer controls which would also close the identified gaps in this research to some extent. This would mean that the gap assessment would have to be done again to ensure compliance with the Cbw. Another potential subject to be researched in the future is PROVES. PROVES is a service which offers Proof of Concept (PoC) pilots and controlled launches of information systems to test information exchange for healthcare innovations. PROVES' goal is to test solutions both technically and functionally from which information can be derived to improve the solutions for real-life usage (Vereniging van Zorgaanbieders voor Zorgcommunicatie, 2024). This could be in combination with new technologies such as AI and IoT opportunities as mentioned in the discussion.

Vendor lock-in is a problem in the healthcare sector. Future research should take this into account.

The NIST CSF as well as COSO were not used as frequently as COBIT and the Good Practice on Information Security by DNB. This had to do with the fact that COBIT and the Good Practice on Information Security were a lot more detailed in specifying formal controls (and thus solutions) for the identified gaps. This is a limitation in the practical

application of the framework, since the controls taken to implement would ideally come evenly distributed from every studied framework.

Despite the experts' similar responses on the majority of controls, there were some deviations in the answers of the experts at certain times. For example, experts 1 and 2 said that they would prefer a simultaneous training for management combined with other types of employees, such as juniors. Most interviewees stated that a separate training for management was necessary, but this was thus not the case for every interviewee. In future research, methods to quantify the data better could be used, such as the Content Validity Index (CVI)[11]. By using the CVI, the data saturation could be improved even further.

A few minor differences in answers also occurred in the two validation interviews. An example of this is gap 6 regarding supply chain cybersecurity. Expert 11 stated that the IT department does not need a say in the final agreement on a new software/application partner, since this is not realistic. Expert 9 stated that this already happens on a small scale; and that having IT more specifically involved in this process is actually a good thing. Since sometimes small deviations between the answers in the validation interviews occurred, it has been chosen to always choose 'the middle ground'. Future research needs to have a higher volume of validation interviews until the point of data saturation is reached. Having spoken to only eleven different experts (ten different experts for the verification, two different experts for the validation of the controls. One of the experts has been spoken with twice) is a limitation in itself. Especially validating the controls' frequencies, despite being checked already in the verification interviews, needs more experts to reach a similar level of data saturation similar to the verification interviews. A rather company biased, homogeneous environment has been used for the research with having only experts within BDO interviewed. Future research should take more different experts and companies in scope.

No distinguishing has been done between the different types of healthcare organizations, such as GPs and the pharmaceutical industry. Neither have differences been made between private and public hospitals. The same applies to comparing the healthcare sector in the Netherlands with other nations, since the Dutch culture regarding NIS2 compliance could be different compares to other EU member states. Future research should take this into account.

The internet consultation of the Cbw has been closed. The Dutch government is currently working on the 'algemene maatregelen van bestuur' which translates to a more detailed elaboration on the Cbw with the improvement suggestions worked out (Ministerie van Economische Zaken en Klimaat, 2024). In future research this documentation should also be taken in scope for updating the framework.

---

[11] This method can be used to create cutoff points for certain statements, which can in turn be used for the validation and coherence of answers given by the interviewed experts (Polit & Beck, 2004).

8 Conclusion

The aim of the research was to develop a framework to help healthcare organizations in the Netherlands to properly prepare to be in compliance with the NIS2 Directive. Compliance is not only important for preventing big fines, but also for the defense and protection of the health of patients. This was done by the creation of a NIS2 compliance framework. Therefore, the following research questions was created:

"*How can the health sector in The Netherlands be assessed to determine whether they are compliant with the NIS2-directive*?"

In order to answer the research question, four sub questions were created. The following overview shows the methods and main conclusion for each sub question.

Sub-question	Method	Main conclusion
"*What measures are organizations in the healthcare sector currently taking to prepare for NIS2?*"	NIS2 in context chapter, literature review chapter, expert interviews	NEN 7510 is the security standard, but is not always fully implemented. Healthcare organizations work conform or similar to NEN 7510. They are not sufficiently prepared for NIS2 compliance and even less for cybersecurity incidents. Incident response is done an ad-hoc.
"*What are the differences in the obligations within NIS2 among organizations in the healthcare sector?*"	NIS2 in context chapter, literature review chapter, expert interviews	The healthcare organization is considered essential according to NIS2. This means that proactive supervision regarding compliance will be done. Hospitals are more likely to be targeted and potential victims of cybercrime, which is why they need more cybersecurity controls in comparison to other healthcare organizations.
"*Which parts of current audit frameworks are useful to develop a NIS2-compliance framework for the healthcare sector*?"	Literature review chapter, current framework analysis chapter	The most used frameworks within IT audit are COSO, COBIT, ITIL, the Good Practice on Information Security from DNB, and the NIST CSF. The controls presented in these frameworks are used in IT auditing. These frameworks were researched in detail for the NIS2 framework.
"*Which risks should be covered by a new NIS2-compliance framework to properly assess the current status (maturity level) of different types of healthcare organizations?*"	NIS2 in context chapter, literature review, current framework analysis chapter, expert interviews	There are six gaps between NEN 7510 and NIS2 which require controls. These are 1) incident management, 2) standardized reporting, 3) contact with the CSIRT, 4) standardized impact assessment, 5) mandatory cybersecurity risk education for management, and 6) supply chain cybersecurity assessment. Hospitals require more controls and sometimes a higher frequency of specific controls due to a higher risk of becoming victim of cybersecurity incidents. This is worked out in the framework through maturity levels.

Table 8: Overview of methods and conclusions of the four sub questions

The answer to the research question is a gap analysis between NEN 7510 and NIS2 where specific controls need to be implemented. The recommendation for all healthcare organizations is to start implementing the dedicated controls based on their corresponding maturity level as soon as possible, since the deadline for mandatory compliance with the NIS2 Directive is the 17th of October, 2024.

References

AACA. (n.d.). *The pros and cons of advisory reports*. aacaglobal.com. https://www.accaglobal.com/gb/en/member/sectors/internal-audit/our-publications/the-pros-and-cons-of-advisory-reports.html

Adams, W. (2015). *Conducting Semi-Structured Interviews* (4th ed.). Jossey-Bass. https://doi.org/10.1002/9781119171386.ch19

Almulihi, A., Alassery, F., Asif, K., Sarita, S., Kumar, G., & Kumar, R. (2022). Scopus preview - Scopus - Welcome to Scopus. *Intelligent Automation and Soft Computing*, *32*(3), 1763–1779. https://www.scopus.com/record/display.uri?eid=2-s2.0-85122210245&origin=inward&txGid=4004eb8d9be7d4f3a4b44fb4876dec71

Amazon. (2024). *Stephen D. Gantz*. amazon.com. https://www.amazon.com/stores/author/B00ATC7M8W/about

Andrade, C. (2018). Internal, External, and Ecological Validity in Research Design, Conduct, and Evaluation. *Indian Journal of Psychological Medicine*, 498–499. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6149308/

Arfaoui, A., Kribèche, A., & Senouci, S. (2019). Context-aware anonymous authentication protocols in the internet of things dedicated to e-health applications. *Computer Networks*, *159*, 23–36. https://doi.org/10.1016/j.comnet.2019.04.031

Averitt, A., Ryan, P., Weng, C., & Perotte, A. (2021). A conceptual framework for external validity. *Journal of Biomedical Informatics*, *121*, 103870. https://doi.org/10.1016/j.jbi.2021.103870

Bailey, E., & Becker, J. (2014). A comparison of IT governance and control frameworks in cloud computing. *Twentieth Americas Conference on Information Systems*, 1825–1840.

BDO. (2024, May 14). *De "gap" tussen NIS2 en ISO27001* [Slide show; Intern]. Vaktechnisch Overleg, Netherlands.

Beulen, E., & Ribbers, P. (2021). *Managing Information Technology Outsourcing* (3rd ed.). Routledge.

Bongiovanni, I., Gale, M., & Slapničar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Brewer, J., & Hunter, A. (2006). *Foundations of Multimethod Research*. Sage Publications Inda Pvt. Ltd.

Broderick, J. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26–31. https://doi.org/10.1016/j.istr.2005.12.001

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical study of Rationality-Based Beliefs and Information Security Awareness on JSTOR. *MIS Quarterly*, *34*(3), 524–548. https://www.jstor.org/stable/25750690

Cascavilla, G. (2023, October). *Cybersecurity Risk Management Lecture*. Cybersecurity Risk Management Lecture - TiSEM, Tilburg, Netherlands.

Centraal Bureau voor de Statistiek. (n.d.). *Welke branches vallen onder de sector zorg en welzijn?* Centraal Bureau Voor De Statistiek. https://www.cbs.nl/nl-nl/faq/arbeidsmarkt-zorg-en-welzijn/welke-branches-vallen-onder-de-sector-zorg-en-welzijn-

Chartered Institute of Internal Auditors. (2023, February 1). Consultancy engagements. *Chartered Institute of Internal Auditors*. https://www.iia.org.uk/resources/delivering-internal-audit/consultancy-engagements/?downloadPdf=true

Chartered Institute of Procurement & Supply. (n.d.). *Kraljic Matrix*. cips.org. https://www.cips.org/intelligence-hub/supplier-relationship-management/kraljic-matrix#:~:text=The%20Kraljic%20Matrix%20is%20a,development%2C%20and%20minimise%20supply%20disruption.

Cliendo. (2023, September 13). *ECD: Elektronisch Clienten Dossier - Cliendo*. https://www.cliendo.nl/ecd-elektronisch-clienten-dossier/

Coker, D. (2023). An Integrative Qualitative Framework: Improving Research Through Strategic Mapping. *International Research in Education*, *11*(1), 66–109. https://doi.org/10.5296/ire.v11i1.20921

Committee of Sponsoring Organizations of the Treadway Commission. (2016). *Enterprise Risk Management—Aligning Risk with Strategy and Performance*.

Cordella, A., & Iannacci, F. (2010). Information systems in the public sector: The e-Government enactment framework. *Journal of Strategic Information Systems*, *19*(1), 52–66. https://doi.org/10.1016/j.jsis.2010.01.001

Cram, A., & D'Arcy, J. (2023). 'What a waste of time': An examination of cybersecurity legitimacy. *Information Systems Journal (Print)*, *33*(6), 1396–1422. https://doi.org/10.1111/isj.12460

Cram, A., D'Arcy, J., & Benlian, A. (2024). Time will tell: The case for an idiographic approach to behavioral cybersecurity research. *MIS Quarterly*, *48*(1), 95–136. https://doi.org/10.25300/MISQ/2023/17707

Cram, A., Proudfoot, J., & D'Arcy, J. (2020). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*(4), 521–549. https://doi.org/10.1111/isj.12319

De Nederlandsche Bank. (2023). *Good Practice Informatiebeveiliging 2023*.

De Snoo, R. (2024). *NIS2 webinar: hoe bereid je je voor op NIS2? [Comment on "Vragen over de Cbw"]*. https://www.samendigitaalveilig.nl/

Digital Trust Center. (2023, October 13). *De impact van NIS2 op jouw organisatie* [Video]. YouTube. https://www.youtube.com/watch?v=iQdkY-fnp30

Digital Trust Center. (2024, May 21). *Internetconsultatie Cyberbeveiligingswet*. https://www.digitaltrustcenter.nl/nieuws/internetconsultatie-cyberbeveiligingswet

Digitale Overheid. (2024a, January 15). *NIS2-richtlijn NIS2-richtlijn - digitale overheid*. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

Digitale Overheid. (2024b, April 9). *Baseline informatiebeveiliging overheid cybersecurity - digitale overheid*. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/

ENISA. (2023). *ENISA THREAT LANDSCAPE 2023*. https://doi.org/10.2824/782573

ENISA. (2024, March 27). ENISA. https://www.enisa.europa.eu/

European Commission. (2020). *IMPACT ASSESSMENT REPORT on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Cybersecurity-review-of-EU-rules-on-the-security-of-network-and-information-systems_en

European Commission. (2023a, June 29). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs*. digital-

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

European Commission. (2023b, September 14). *Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive)*. digital-strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive

European Parliament. (2022). Directive - 2022/2555 - EN - EUR-LEX. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union. (n.d.). *Types of legislation*. European-union.europa.eu. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

European Union. (2016, July 19). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. EUR-lex.europa.eu. https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Fu, A. (2022, October 23). *What is the difference between EMR and EHR?* UniPrint.net. https://www.uniprint.net/en/difference-between-emr-ehr/

Fusch, P., & Ness, L. (2015). Are We There Yet? Data Saturation in Qualitative Research. *The Qualitative Report*, *20*(9), 1408–1416. https://scholarworks.waldenu.edu/facpubs/455/?utm_campaign=PDFCoverPages&utm_medium=PDF&utm_source=scholarworks.waldenu.edu%2Ffacpubs%2F455

Gantz, S. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information* [Google Scholar]. Elsevier.

GRC International Group. (n.d.). *Software Capability Maturity Model (CMM)*. itgovernance.eu. https://www.itgovernance.eu/sv-se/capability-maturity-model-se

Grobman, S., & Cerra, A. (2016). *The Second Economy* (1st ed.) [Springer link]. Apress Berkeley, CA.

Gulinck, I. (2024, April 29). *Information session on the types of reports within IT Auditing*.

He, Y., Zamani, E., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of*

Information Management, *62*, 102435. https://doi.org/10.1016/j.ijinfomgt.2021.102435

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://www.jstor.org/stable/25148625

Hugo, H. (2023, December 28). Drie Duitse ziekenhuizen staken spoedeisende hulp na ransomwareaanval. *Tweakers*. https://tweakers.net/nieuws/216958/drie-duitse-ziekenhuizen-staken-spoedeisende-hulp-na-ransomwareaanval.html

Inspectie Gezondheidszorg en Jeugd. (2023, November 16). *Ziekenhuizen maken stevige inhaalslag met informatiebeveiliging*. igj.nl. https://www.igj.nl/publicaties/publicaties/2023/11/16/ziekenhuizen-maken-stevige-inhaalslag-met-informatiebeveiliging#:~:text=Bijna%20alle%20ziekenhuizen%20voldoen%20in,dit%20gebied%20aan%20te%20pakken.

International Auditing and Assurance Standards Board. (2013). *ISAE 3000 (revised) assurance engagements other than audits or reviews of historical financial information*. https://www.ifac.org/_flysystem/azure-private/publications/files/ISAE%203000%20Revised%20-%20for%20IAASB.pdf

International Auditing and Assurance Standards Board. (2020). *International Standard on Related Services 4400 (revised)*. https://www.ifac.org/_flysystem/azure-private/publications/files/ISRS-4400-Revised-Agreed-Upon-Procedures-final.pdf

International Electrotechnical Commission. (n.d.). *Understanding standards*. iec.ch. https://www.iec.ch/understanding-standards

ISACA. (n.d.). *Effective IT Governance at Your Fingertips*. ISACA.org. https://www.isaca.org/resources/cobit

ISACA. (2012a). *COBIT 5 - enabling processes*.

ISACA. (2012b). COBIT 5 A Business Framework for the Governance and Management of Enterprise IT. In *Isaca.org*.

ISACA. (2018). Introducing COBIT 2019 overview. In *isaca.org*. https://www.isaca.org/resources/cobit

ISO/IEC 27001:2022. (n.d.). ISO. https://www.iso.org/standard/27001

ITIL open guide. (n.d.). *ITIL*. itillibrary.org. https://www.itlibrary.org/

Jalali, M., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems*, *28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Kamara, I., & Van Den Boom, J. (2022). *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices*. https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2022/october/13/index/NCSC_NIS2_D1_Final.pdf

Khansa, L., Cook, D., James, T., & Bruyaka, O. (2012). Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *Computers & Security*, *31*(6), 750–770. https://doi.org/10.1016/j.cose.2012.06.007

Kohnke, A., Sigler, K., & Shoemaker, D. (2017). *Implementing Cybersecurity INTERNAL AUDIT AND IT AUDIT SERIES Implementing Cybersecurity A Guide to the National Institute of Standards and Technology Risk Management Framework*. Taylor 7 Francis Group.

Kolouch, J., Zahradnický, T., & Kučínský, A. (2021). CYBER SECURITY: LESSONS LEARNED FROMCYBER-ATTACKS ON HOSPITALS IN THE COVID-19 PANDEMIC. *Masaruk University Journal of Law and Technology*, *15*(2). https://journals.muni.cz/mujlt/article/view/14463/12356

Kreutzer, M., Cardinal, L., Walter, J., & Lechner, C. (2016). Formal and Informal Control as Complement or Substitute? The Role of the Task Environment. *Stragegy Science*, *1*(4). https://pubsonline.informs.org/doi/full/10.1287/stsc.2016.0019

Krüger, C., & Johnson, R. (2010). Information management as an enabler of knowledge management maturity: A South African perspective. *International Journal of Information Management*, *30*(1), 57–67. https://doi.org/10.1016/j.ijinfomgt.2009.06.007

Larsen, K., Lukyanenko, R., Mueller, R., Storey, V., Van Der Meer, D., Parsons, J., & Hovorka, D. (2020). Validity in Design Science Research. *15th International Conference on Design Science Research in Information Systems and Technology*, 272–282.

Lean Six Sigma Groep. (n.d.). *What does RACI mean?* leansixsigmagroep.nl. https://leansixsigmagroep.nl/en/lean-agile-and-six-sigma/raci/

Leino, T. (2024, January 31). *Lecture 1 week 4 - ITG and ITSM*. ITG And ITSM Class - Turku School of Economics, Turku, Finland.

Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry* [Google Scholar]. SAGE publications, inc.

Maier, A., Moultrie, J., & Clarkson, J. (2012). Assessing Organizational Capabilities: Reviewing and Guiding the Development of Maturity Grids. *IEEE Transactions on Engineering Management*, *59*(1), 138–159. https://www.researchgate.net/publication/224247221_Assessing_Organizational_Capabilities_Reviewing_and_Guiding_the_Development_of_Maturity_Grids

Malatji, M. (2023, January 26). *Management of enterprise cyber security: A review of ISO/IEC 27001:2022*. IEEEXplore.ieee.org. https://ieeexplore.ieee.org/abstract/document/10051114

Mamdouh, M., Awad, A., Khalaf, A., & Hamed, H. (2021). Authentication and Identity Management of IOHT Devices: Achievements, challenges, and future directions. *Computers & Security*, *111*, 102491. https://doi.org/10.1016/j.cose.2021.102491

Marett, K., & Nabors, M. (2021). Local learning from municipal ransomware attacks: A geographically weighted analysis. *Information & Management (Amsterdam)*, *58*(7), 103482. https://doi.org/10.1016/j.im.2021.103482

McIntosh, T., Liu, T., Sušnjak, T., Alavizadeh, H., Ng, A., Nowrozy, R., & Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: A focus on ransomware attack mitigation. *Computers & Security*, *134*, 103424. https://doi.org/10.1016/j.cose.2023.103424

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, *136*, 103489. https://doi.org/10.1016/j.cose.2023.103489

Ministerie van Algemene Zaken. (2023, June 5). *Wet beveiliging netwerk- en Informatiesystemen (Wbni) voor digitale dienstverleners*. Rijksoverheid.nl. https://www.rijksoverheid.nl/documenten/rapporten/2018/09/01/wet-beveiliging-netwerk--en-informatiesystemen-wbni-voor-digitale-dienstverleners

Ministerie van Economische zaken en klimaat. (n.d.). *Wet beveiliging netwerk- en informatiesystemen (Wbni)*. Digital Trust Center (Min. Van EZK). https://www.digitaltrustcenter.nl/wet-beveiliging-netwerk-en-informatiesystemen-wbni#:~:text=Wat%20betekent%20de%20Wbni%20voor,gelden%20er%20een%20aantal%20verplichtingen

Ministerie van Economische Zaken en Klimaat. (2023, July 3). *Samenhangend Inspectiebeeld cybersecurity vitale processen 2023*. rdi.nl. https://www.rdi.nl/documenten/rapporten/2023/07/03/samenhangend-inspectiebeeld-cybersecurity-vitale-processen-2023

Ministerie van Economische Zaken en Klimaat. (2024, July 3). *Internetconsultatie Cyberbeveiligingswet (NIS2) gesloten*. digitaltrustcenter.nl. https://www.digitaltrustcenter.nl/nieuws/internetconsultatie-cyberbeveiligingswet-nis2-gesloten

Ministerie van Volksgezondheid, Welzijn en Sport. (2023, May 22). *Vragen over NEN 7510*. gegevensuitwisselingindezorg.nl. https://www.gegevensuitwisselingindezorg.nl/weerbaarheid/vragen-en-antwoorden

MKB-Nederland. (2024). *MKB-Nederland: voor een kansrijk ondernemersklimaat!* mkb.nl. https://mkb.nl/over-mkb-nederland

Moeller, R. (2011). *COSO Enterprise Risk Management*. John Wiley & Sons, inc.

Mukhopadhyay, A., & Jain, S. (2024). A framework for cyber-risk insurance against ransomware: A mixed-method approach. *International Journal of Information Management*, *74*, 102724. https://doi.org/10.1016/j.ijinfomgt.2023.102724

National Institute of Standards and Technology. (2018). *Risk Management Framework for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

Nedap. (2023, November 9). *Nedap Healthcare - Samen werken aan betere zorg*. Nedap Healthcare. https://nedap-healthcare.com/

NEN. (n.d.-a). *NEN 7510: Informatiebeveiliging in de zorg*. nen.nl. https://www.nen.nl/zorg-welzijn/ict-in-de-zorg/informatiebeveiliging-in-de-zorg

NEN. (n.d.-b). *Over NEN*. nen.nl. https://www.nen.nl/over-nen

NEN. (n.d.-c). *Vrij beschikbare normen door dwingende verwijzing in wetgeving*. nen.nl. https://www.nen.nl/Over-NEN/Vrij-beschikbare-normen

NEN. (2017). *NEN 7510-2_2017*. https://www.nen.nl/nen-7510-2-2017-nl-238787

NEN. (2020, February 20). *NEN 7510-1:2017+A1:2020 nl*. nen.nl. Retrieved April 2, 2024, from https://www.nen.nl/en/nen-7510-1-2017-a1-2020-nl-267179

NIST. (2006). *FIPS 200*. NIST Computer Security Reesource Center. https://csrc.nist.gov/pubs/fips/200/final

NOREA. (n.d.). *De beroepsorganisatie van IT-auditors*. Norea.nl. https://www.norea.nl/

NOREA. (2021). Handreiking voor SOC 2® en SOC 3® op basis van ISAE3000 / richtlijn 3000A. In *norea.nl*. https://www.norea.nl/handreikingen

NOREA. (2022, September 22). *Consultatie herziening Richtlijn 4401*. norea.nl. https://www.norea.nl/nieuws/consultatie-herziening-richtlijn-4401

NOS. (2020, February 5). Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald. *NOS*. https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaald

Object Management Group. (2024). *Business Process Model and Notation - Home*. bpmn.org. https://www.bpmn.org/

Ogbanufe, O., Kim, D., & Jones, M. (2021). Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. *Information & Management*, *58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507

Overheid.nl. (2024). *NIS2 wetsvoorstel consultatieversie*. https://www.internetconsultatie.nl/cyberbeveiligingswet/document/12561

Palilingan, V., & Batmetan, J. (2018). Incident management in Academic Information System using ITIL Framework. *IOP Conference Series: Materials Science and Engineering*, 306. https://doi.org/10.1088/1757-899X/306/1/012110

Patton, M. (2005). Qualitative research. *Encyclopedia of Statistics in Behavioral Science*. https://doi.org/10.1002/0470013192.bsa514

Polit, D., & Beck, C. (2004). *Nursing research: principles and methods* (7th ed.) [WorldCat]. Lippincott Williams & Wilkins. https://search.worldcat.org/title/Nursing-research-:-principles-and-methods/oclc/51304384

Reeves, A., Calic, D., & Delfabbro, P. (2023). “Generic and unusable”1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security*, *128*, 103137. https://doi.org/10.1016/j.cose.2023.103137

Rijksinspectie Digitale Infrastructuur. (n.d.). *Wet beveiliging netwerk- en informatiesystemen (Wbni)*. rdi.nl. https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen

Rijksoverheid. (2024, February 29). *NIS2 Quickscan*. https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/

Roodhooft, W. (2024). Healthcare cybersecurity: Our hospital’s path to better cyber resilience. *CIO : The Magazine for Information Executives*, *1*(1328–4045), 240907785.

Samen Digitaal Veilig. (2024). *Nu al een NIS2 Quality Mark?* samendigitaalveilig.nl. https://www.samendigitaalveilig.nl/nu-al-een-nis2-quality-mark/

Schmeelk, S. (2022). Computer-Mediated communication [Google Books]. In *Google Books*. IntechOpen. https://books.google.fi/books?hl=en&lr=&id=XrdaEAAAQBAJ&oi=fnd&pg=PA77&dq=%22healthcare+IT+risk%22&ots=xGBIyMg3T0&sig=ubVdXW5SQrsO524lQ-bEoeYFM4g&redir_esc=y#v=onepage&q=%22healthcare%20IT%20risk%22&f=false

Schmeelk, S., Dragos, D., & DeBello, J. (Eds.). (2021). What Can We Learn about Healthcare IT Risk from HITECH? Risk Lessons Learned from the US HHS OCR Breach Portal. *Proceedings of the 54th Hawaii International Conference on System Sciences*. https://hdl.handle.net/10125/71101

Scully, T. (2014). The cyber security threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning*, *7*(2), 138–148.

Spiteri, I. (2023, November 8). *NIS2 Directive and DORA - BDO Malta*. https://www.bdo.com.mt/en-gb/insights/the-relationship-between-nis-2-directive-and-dora

Stichting Kwaliteitsinnovatie. (2024). *De norm*. nis2qualitymark.eu. https://nis2qualitymark.eu/keurmerk/

Sushma, K., Viji, C., Rajkumar, N., Ravi, J., Stalin, M., & Najmusher, H. (2023). Healthcare 4.0: A review of phishing attacks in Cyber security. *Procedia Computer Science*, *230*, 874–878. https://doi.org/10.1016/j.procs.2023.12.045

Tarikere, S., Donner, I., & Woods, D. (2021). Diagnosing a healthcare cybersecurity crisis: The impact of IoMT advancements and 5G. *Business Horizons*, *64*(6), 799–807. https://doi.org/10.1016/j.bushor.2021.07.015

Tejay, G., & Mohammed, Z. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3), 103751. https://doi.org/10.1016/j.im.2022.103751

The Audit Generation. (n.d.). *Rapport van feitelijke bevindingen*. theauditgeneration.nl. https://theauditgeneration.nl/diensten/rapport-feitelijke-bevindingen/

The NIS2 Directive. (2023a, March 3). *Why NIS2?* https://nis2directive.eu/why-nis2/

The NIS2 Directive. (2023b, March 7). *NIS2 Fines*. nis2directive.eu. https://nis2directive.eu/nis2-fines/

The NIS2 Directive. (2023c, March 10). *NIS2 Requirements*. nis2directive.eu. https://nis2directive.eu/nis2-requirements/

Thomasian, N., & Adashi, E. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, *10*(3), 100549. https://doi.org/10.1016/j.hlpt.2021.100549

Tilburg University. (2023, October 20). *List of good IM journals*. Canvas.com. https://tilburguniversity.instructure.com/courses/4629/pages/5-list-of-good-im-journals?module_item_id=59750

Tin, D., Hata, R., Granholm, F., Ciottone, R., Staynings, R., & Ciottone, G. (2023). Cyberthreats: A primer for healthcare professionals. ˜ *the œAmerican Journal of Emergency Medicine*, *68*, 179–185. https://doi.org/10.1016/j.ajem.2023.04.001

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: a cybersecurity frameworks review. *Journal of Industrial Information Integration*, 100604. https://doi.org/10.1016/j.jii.2024.100604

Turner, D. (2010). Qualitative Interview Design: a practical guide for novice investigators. *The Qualitative Report*, *15*(3), 754–760. https://doi.org/10.46743/2160-3715/2010.1178

Van Der Meulen, N. (2013). DigiNotar: Dissecting the first Dutch digital disaster. *Journal of Strategic Security*, *6*(2), 46–58. https://digitalcommons.usf.edu/jss/vol6/iss2/4/

Van Der Vliet, A. (2022). *Business Research Techniques for Premaster* [Slide show; Tilburg University Canvas].

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890. https://doi.org/10.1016/j.clsr.2023.105890

Vereniging van Zorgaanbieders voor Zorgcommunicatie. (2024). *Proves*. vzvz.nl. https://www.vzvz.nl/diensten/gemeenschappelijke-diensten/proves

Verlaan, D. (2022, April 6). *Woningcorporaties gehackt, ID-bewijzen en bankgegevens op straat*. RTL Nieuws. https://www.rtlnieuws.nl/tech/artikel/5299889/conti-ransomware-cybercriminelen-aanval-woningcorporaties

VNO-NCW. (2024). *Wat is VNO-NCW?* vno-ncw.nl. https://www.vno-ncw.nl/over-vno-ncw

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, *52*, 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Wieringa, R. (2014). Design Science Methodology for information systems and software engineering. In *Springer eBooks*. https://doi.org/10.1007/978-3-662-43839-8

XIS Keurmerk. (2024). *Over het XIS Keurmerk*. xiskeurmerk.nl. https://xiskeurmerk.nl/over-ons/

Yeşilgöz-Zegerius, D., Eerdmans, J., & Jetten, R. (2024). Antwoord op vragen van het het lid Eerdmans over ‘de (cyber)veiligheid van Nederlandse offshore olie- en gasplatforms.’ In *Tweedekamer.nl*. Tweede Kamer. https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2024D21855&did=2024D21855

Appendices

Appendix 1: Organizations with jurisdiction of the Member State in which their main establishment is

When organizations span multiple borders, it can be confusing which authority has jurisdiction over them. The country in which the organization has their main office, is regarded as the country which has jurisdiction over the organization. ENISA will keep a register of this. Even if the main establishment is not in Europe, it still has to deal with NIS2. The idea is that these organizations don't have to deal will several legal implications. The list is as follows:

- Domain name service providers;
- Top level domain name registries;
- Organizations providing domain name registration services;
- Cloud computing service providers;
- Data center service providers;
- Content delivery network providers;
- Managed service providers;
- Managed security service providers;
- Providers of online marketplaces;
- Providers of search engines;
- Providers of social networking platforms (European Commission, 2023a).

Appendix 2: List of good IM-journals according to Tilburg University

Tilburg University (2023) offers a list of good IM-journals, which is often referred to as 'the basket of 8' or a similar number as 8 which represents a list of top-core, top and very good Information Management journals. The list is as follows:

Top-core:

- ACM Transactions on Information Systems Information Systems
- Information Systems Research
- INFORMS Journal on Computing
- Management Science Europe
- MIS Quarterly

Top:

- ACM Computing Surveys
- European Journal of Information Systems
- IEEE Transactions on Knowledge and Data Engineering
- Journal of the Association for Information Systems

- Journal of Strategic Information Systems
- VLDB Journal

Very good:

- ACM Transactions on the Web
- CAiSE Proceedings
- Communications of the ACM
- Data and Knowledge Engineering
- Decision Support Systems
- ECIS Proceedings
- Electronic Markets
- IEEE Software
- IEEE Transactions on Software Engineering
- Information and Management
- Information and Software Technology
- Information Systems Journal
- International Journal of Electronic Commerce
- Journal of Group Decision and Negotiation
- Journal of Information Technology
- Journal of MIS
- Journal of Systems and Software
- Requirements Engineering Journal
- Wirtschaftsinformatik
- World Wide Web Journal

Appendix 3: Example risk matrix

Mukhopadhyay and Jain (2024) have created a risk assessment matrix based on a two by two risk-severity heat matrix. Each data point represents the exposure to a specific risk due to a ransomware attack. An example by Mukhopadhyay and Jain (2024) is as follows:

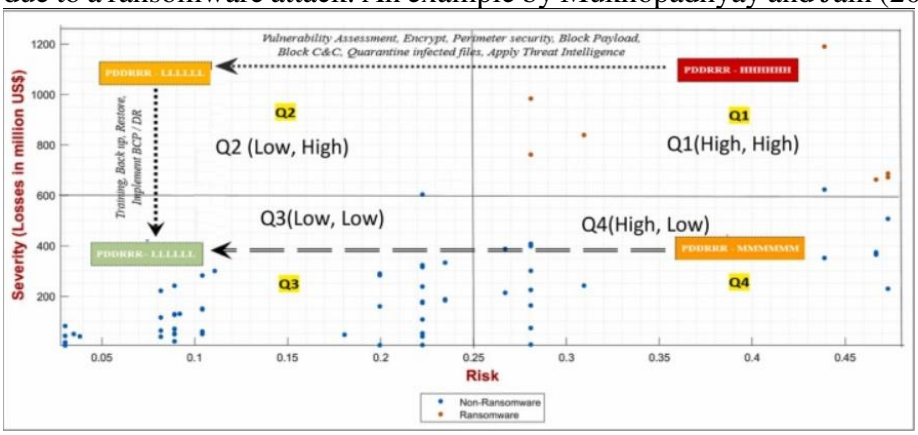


Figure 13: An example risk matrix by Mukhopadhyay and Jain (2024)

Appendix 4: Demonstrating reliability and validity

Criteria	Techniques	
Credibility (internal validity)	1) Prolonged engagement 2) Persistent observation 3) Triangulation (sources, methods, investigators) 4) Peer debriefing 5) Negative case analysis 6) Referential adequacy (archiving of data) 7) Member checks	(pp. 301-304) (pp. 304-305) (pp. 305-307) (pp. 308-309) (pp. 309-313) (pp. 313-314) (pp. 314-316)
Transferability (external validity)	8) Thick description	(p. 316)
Dependability (reliability)	9) Overlap methods (Triangulation of methods) 10) Dependability audit - examining the process of the inquiry (how data was collected; how data was kept; accuracy of data)	(p. 317) (pp. 317-318)
Confirmability (objectivity)	11) Confirmability audit - examines the product to attest that the findings, interpretations & recommendations are supported by data	(pp. 318-327)
All 4 criteria	12) Reflexive journal (about self & method)	(p. 327)

Figure 14: Techniques to demonstrate reliability and validity (Lincoln & Guba, 1985).

Appendix 5: COBIT enabler 1: principles, policies and frameworks

The first enabler of COBIT is created so that the wanted behavior is translated into useful guidance for everyday management. Principles and policies refer to "*the communication mechanisms put into place to convey the governing bodies and management's direction and instructions*" (ISACA, 2012b, p. 67). The first enabler describes four dimensions, which are stakeholders, goals, life cycle, and good practices. Below, an overview and explanation of the four dimensions is presented (ISACA, 2012b).

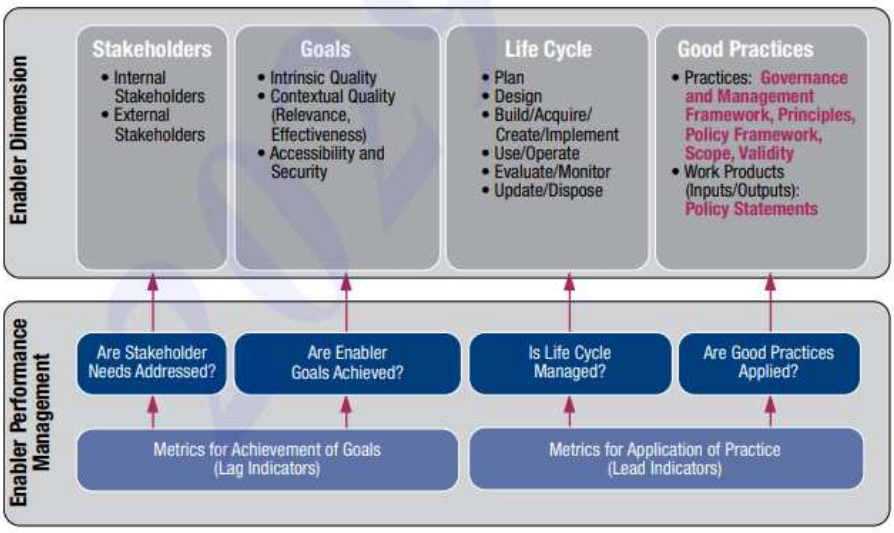


Figure 15: Enabler 1 of COBIT in detail: principles, policies and frameworks (ISACA, 2012b).

Stakeholders

Stakeholders for principles and policies can be internal as well as external to an organization. Stakeholders includes compliance officers, the BoDs and executive management, risk managers, internal and external auditors, among others. The stakes move both ways: certain stakeholders may define and create policies, where other stakeholders have to comply with policies or align with them (ISACA, 2012b).

Goals and metrics

Principles, policies and frameworks are also ways to communicate the obligations of the organization, to support the governance goals and organizational values. These are defined by the executive management and the board. Principles need to be created in simple language, where the core values of the organization are explained as clearly as possible. They also need to be limited in number. This means that there should not be too many principles in place (ISACA, 2012b).

Policies help with explaining guidance in more detail on how to put the created principles into practice. Policies also influence how decision making aligns with the created principles. Good policies are 1) effective (they should achieve the stated goal), 2) efficient (they should ensure that the implementation of the principles is done in an efficient manner), and 3) non-intrusive (they should be logical for the people who have to comply with them. This means that no unnecessary resistance is created). Finally, policies should be easily accessible. Finding the policies should not be difficult for the stakeholders (ISACA, 2012b).

Governance and management frameworks have to help management with sufficient governance and management of enterprise IT. Frameworks created should be 1) comprehensive (all necessary areas should be covered), 2) open and flexible (adaptation to the organization's specific situation should be possible), 3) current (the current direction of the organization as well as the current governance objectives should be reflected), and 4) available (the frameworks should be accessible and available to all stakeholders) (ISACA, 2012b).

Life cycle

Policies all have a life cycle. These cycles have to support the reaching of the goals set. Frameworks are key in providing structures to define consistent guidance. Dependent on the external environment in which the organization is present, different degrees of regulatory requirements for strong internal controls is needed. This results in the requirement of a strong policy framework. It is key to review and update policies frequently, as well as checking if there sufficient mechanisms present to ensure awareness among people (ISACA, 2012b).

Good practices

Good practices requires that policies are part of generic management and governance frameworks. Good practices have to provide a (hierarchical) structure wherein all policies have to fit in. Good practices also have to make clear links to the underlying principles. Within good practices, several things have to be described. These are 1) the scope and

validity, 2) the consequences of not complying with the created policies, 3) the ways for handling exceptions within the policy, and 4) the ways in how compliance with the policy is measured and checked.

Finally, policies should be aligned with the amount of risk an organization is willing to take. This risk appetite has to be reflected in the policies. For example, a more risk-averse organization has stricter policies than a risk-aggressive organization. The policies should be evaluated and updated regularly over time (ISACA, 2012b).

Appendix 6: COBIT enabler 2: processes

The second enabler describes a set of activities and practices to achieve certain objectives. This enabler also produces a set of outputs to support the achievement of overall IT-related goals (ISACA, 2012b). ISACA defines a process as "*a collection of practices influenced by the enterprise's policies and procedures that takes inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g., products, services)*" (ISACA, 2012b, p. 69). The second enabler of COBIT is presented visually below:

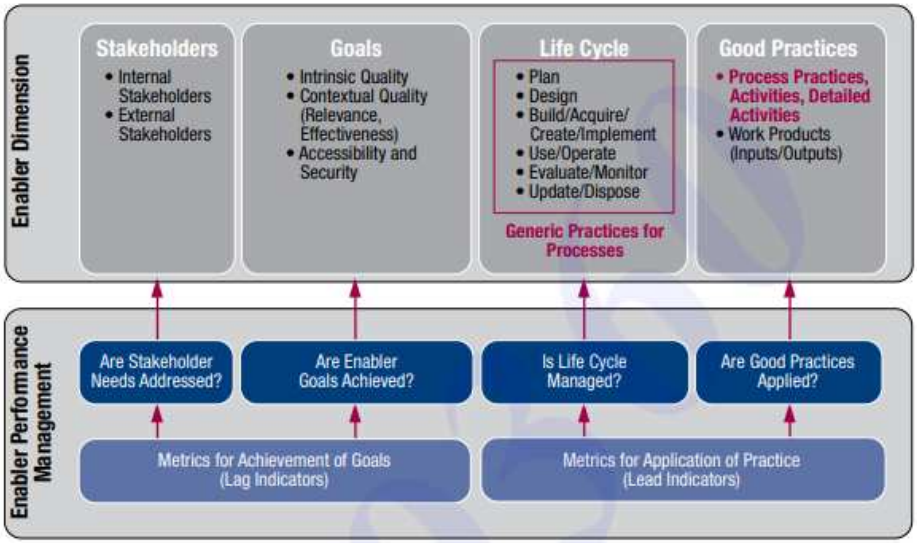


Figure 16: Enabler 2 of COBIT in detail: processes (ISACA, 2012b).

The process models shows that stakeholders have internal and external stakeholders, as mentioned in the first enabler. Each stakeholder has its own role, which is often documented in RACI charts[12]. The process model also shows goals. Process goals are a statement explaining the wanted result of a process. The result can be an artefact, a major change of a state, or a capability improvement which is significant. The process goals

[12] RACI stands for Responsible, Accountable, Consulted and Informed. A RACI chart is often used for writing down the different roles in completing deliverables, goals or tasks within a process or project (Lean Six Sigma Groep, n.d.).

should support IT-related goals. This way, they can help supporting the reaching of goals of an organization (ISACA, 2012b).

Process goals can be categorized as intrinsic goals. The processes need to have intrinsic qualities, they should be accurate and in alignment with good practices, as well as compliant with both internal and external rules. Next to this, process goals can be categorized as contextual goals. The processes should be customized and adapted to the organization's specific situation, as mentioned in the first enabler. The processes should be easy to apply, understand and relevant. Finally, process goals can be categorized as accessibility and security goals. Processes have to be (and stay) confidential, if this is required. The processes should also be known and accessible to the people who need to work with them.

COBIT has created a process reference model which can be used for a starting point to govern IT on an enterprise level. COBIT describes five subsets in their reference model. These are Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA) (ISACA, 2012b). An overview of these processes is presented below:

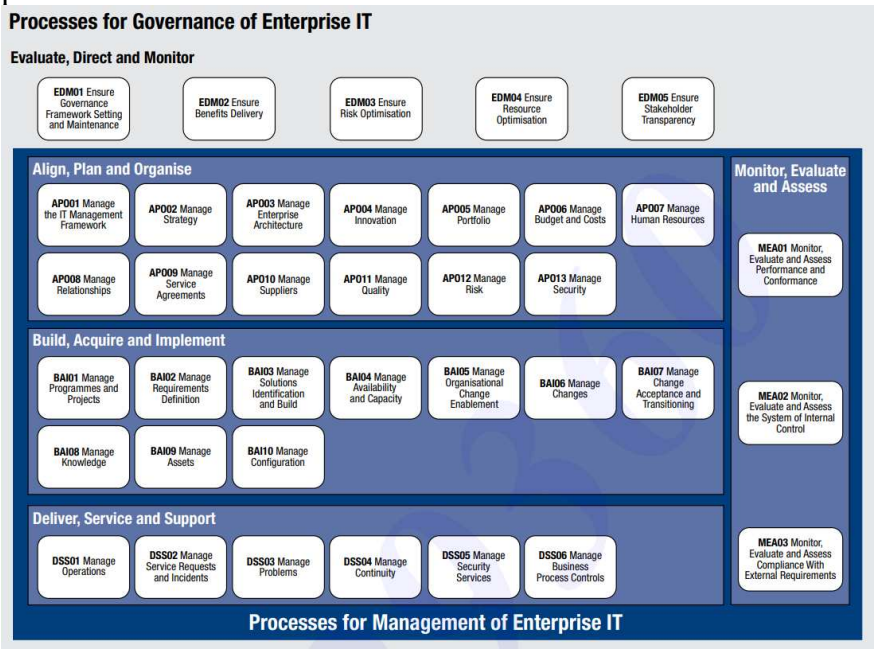


Figure 17: COBIT 5's process reference model (ISACA, 2012b).

Appendix 7: COBIT enabler 3: organizational structures

The third enabler entails key decisions-making within organizational structures. COBIT's organizational structure model shows different parts of the enabler dimensions. The most important parts of this enabler are presented in the good practices. Practices can be 1) operating principles (practical arrangements for the operation of the organizational structure, such as the amount of meetings and documentation), 2) composition

(organizational structures have members, which are internal- and external stakeholders), 3) span of control (the organizational structure's decision rights has certain boundaries set), 4) level of authority (also defined as decision right, since the organizational structure is authorized to make certain decisions), 5) delegation of authority (the organizational structure can delegate the decision rights (or parts of them) to other organizational structures reporting to them), and 6) escalation procedures (escalation paths for an organizational structure have to describe the required tasks in the scenario of problems occurring regarding decision making) (ISACA, 2012b).

The third enabler of COBIT is presented visually below:

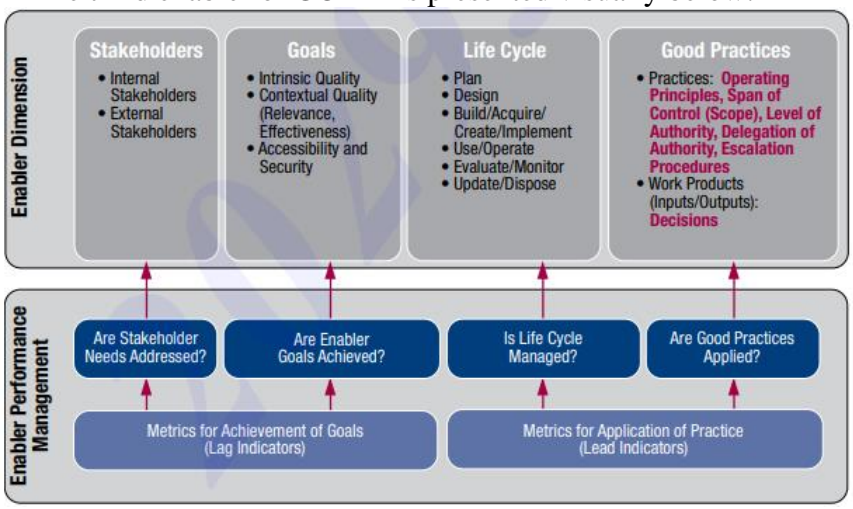


Figure 18: Enabler 3 of COBIT: organizational structures (ISACA, 2012b).

Appendix 8: COBIT enabler 4: culture, ethics and behavior

The fourth enabler describes that individuals within organizations are often underestimated as a success factor, in both management and governance. Good practices regarding the fourth enabler of COBIT includes communication, enforcement, incentives and rewards, awareness, rules and norms, and champions. Regarding the desired behavior and the corporate values within an organization, there should be good practices in place. This also applies to the awareness of the desired behavior. Senior management and other champions should demonstrate this behavior as role models. Next to this, there have to be incentives in place to encourage the desired behavior to be expressed. Finally, rules and norms which can provide guidance in detail on the desired behavior within an organization should be in place. Links to the principles and policies that an organization has created should be very clear (ISACA, 2012b).

The fourth enabler of COBIT is presented visually below:

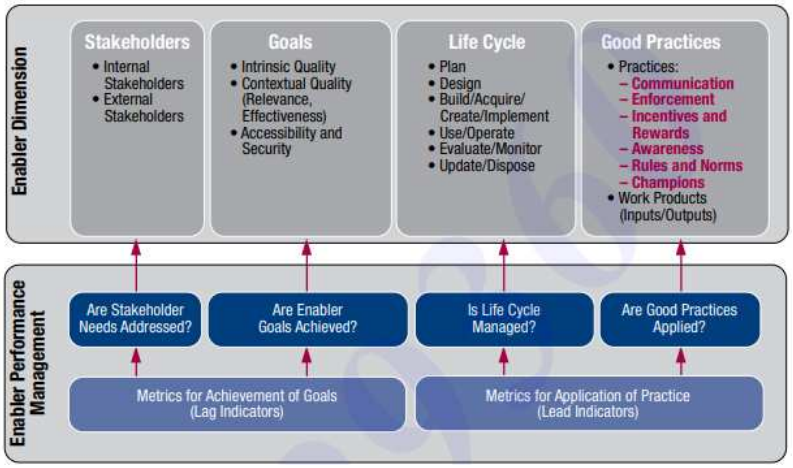


Figure 19: Enabler 4 of COBIT: culture, ethics and behavior (ISACA, 2012b).

Appendix 9: COBIT enabler 5: information

The fifth enabler states that information is pervasive within the entire organization. Information includes all information produced and used within an organization. Information is mandatory for keeping an organization up-and-running as well as well-governed. On an operational level, information is often the key product of an organization itself (ISACA, 2012b).

This enabler deals with all relevant information for organizations. This also applies to non-automated information. The information can be structured or unstructured, formalized or informalized. According to COBIT, information can be considered to be in a certain stage in the so-called 'information cycle' of an organization. Within this cycle, business processes are generating and processing data. After this, they transform the data into information and knowledge. This eventually reaches the state where the organization can derive value from the information and knowledge. An overview of the information cycle is presented below:

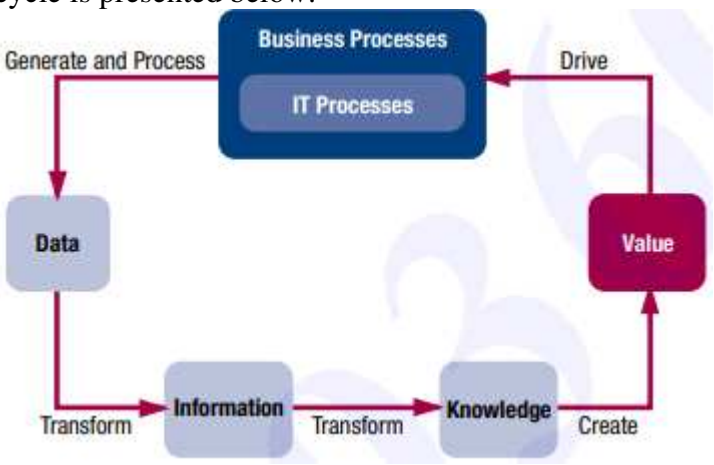


Figure 20: COBIT 5's information cycle (ISACA, 2012b).

The good practices for the information enabler are proposed by COBIT to structure the properties of information. This structure consists of six layers, which defines and describes the properties of information (ISACA, 2012b).

Physical world layer

The first layer is the physical world layer. This layer entails every phenomenon which can be empirically observed. Information carriers or media are attributes which identify the physical carrying of information, such as electronic signals and paper (ISACA, 2012b).

Empiric layer

The second layer entails the empirical observation of the ways used to encode information. The information access channel is an attribute which identifies the ways how to access information, such as user interfaces (ISACA, 2012b).

Syntactic layer

The third layer entails the principles and rules which construct sentences in either natural or artificial language. Code or language is the attribute which identifies the representational language or format which is used for encoding information (ISACA, 2012b).

Semantic layer

The fourth layer entails the rules and principles for deriving certain meaning out of syntactic structures. The information type is the attribute which identifies the type of information, the information currency is the attribute which identifies the time referred to by information (such as if information was in the past, present or future), and the information level is the attribute which identifies the degree of detail that information has (ISACA, 2012b).

Pragmatic layer

The fifth layer entails the rules and structures for constructing language structures which are larger in nature, which fulfils specific goals in the communication among people. Pragmatics are defined as how information is used. The retention period is the attribute of information which identifies how long information can be kept before it is destroyed. The information status attribute identifies if the information is either historical or operational. The novelty attribute identifies whether the information creates new knowledge. It can also confirm existing knowledge. The contingency attribute identifies whether the information can be seen as information or not (ISACA, 2012b).

Social world layer

The final layer explains that the world is socially constructed. This is done by using language structures at the pragmatic level. The context attribute identifies the context in which the information is presented. It looks if information has value for the organization and if it makes sense (ISACA, 2012b).

The fifth enabler of COBIT is presented visually below:

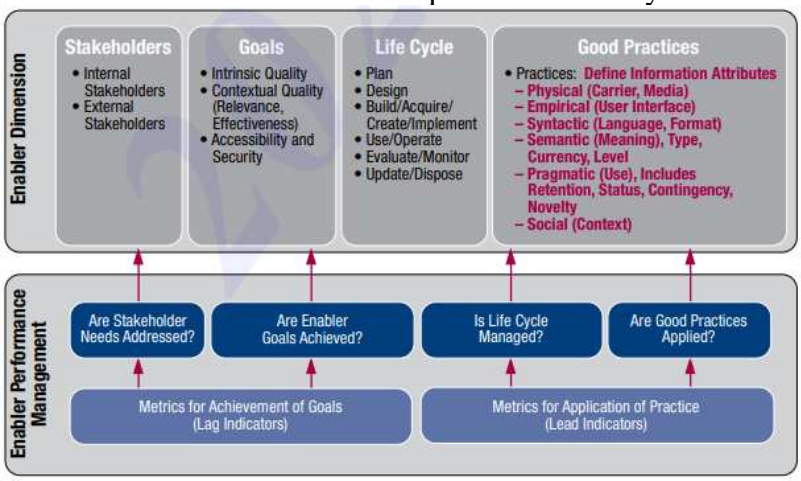


Figure 21: Enabler 5 of COBIT: information (ISACA, 2012b).

Appendix 10: COBIT enabler 6: services, infrastructure and applications

The sixth enabler includes the technology, infrastructure, and applications which provides organization with services and information technology processing.

Both in the goals and good practices dimensions of this enabler, there are elements to highlight.

Firstly, the goals of the enabler are expressed in terms of services, which include applications, infrastructure, technology, and service levels. Next to this, the good practices for service capabilities includes a few definitions. The first definition is that of architecture principles. These are overall guidelines, which help with governing implementations as well as the usage of IT-related resources within organizations. Examples of these good practices are reuse and simplicity. Common parts of the organizational architecture have to be used when creating and implementing solutions as parts for a visualized future architectural state. Simplicity implies that the architecture of organizations is created and maintained in a simple manner, while also meeting the requirements of the organization.

Architecture viewpoints are models, matrices and catalogues which are used for describing the baseline, goals and transition architectures. An application architecture can be described via an interface diagram. This shows the applications which are currently in

use (or applications which will be used in the future). Service levels must be created as well as achieved by the providers of services which an organization collaborates with.

Reference repositories are external good practices regarding architecture frameworks. These can be templates, guidelines or standards. Using (a combination of) these can help with quickly improving the current organizational architecture. Examples which can be used for this are TOGAF and ITIL (ISACA, 2012b).

The sixth enabler of COBIT is presented visually below:

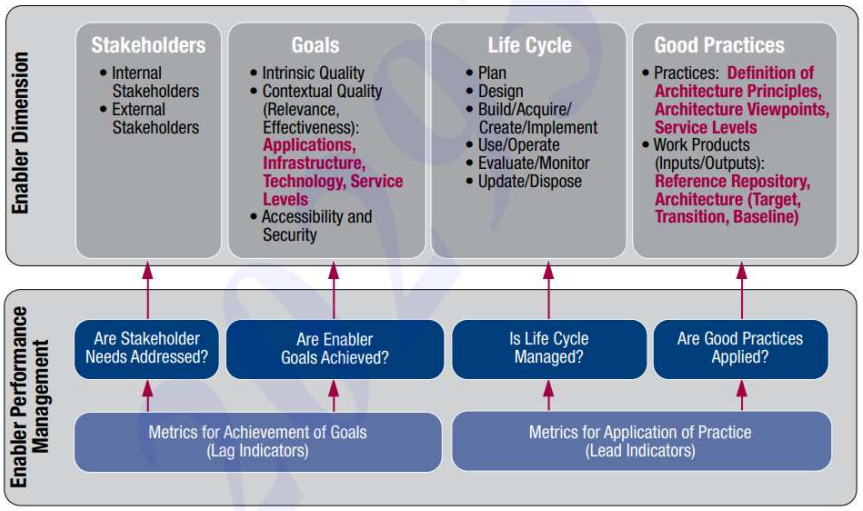


Figure 22: Enabler 6 of COBIT: services, infrastructure and applications (ISACA, 2012).

Appendix 11: COBIT enabler 7: people, skills and competencies

The final enabler mentions that people, skills and competencies are connected to other people. People with proper skills and competencies are a necessity for the successful completion of all activities within an organization. People are also required for not making mistakes in decisions, as well as for taking corrective actions. Highlights of the seventh enabler are within the goals and good practices dimensions. For the goals dimension, education and qualification as various types of skills are important for the successful performance of process activities and roles within the organization (ISACA, 2012b). The seventh enabler of COBIT is presented visually below:

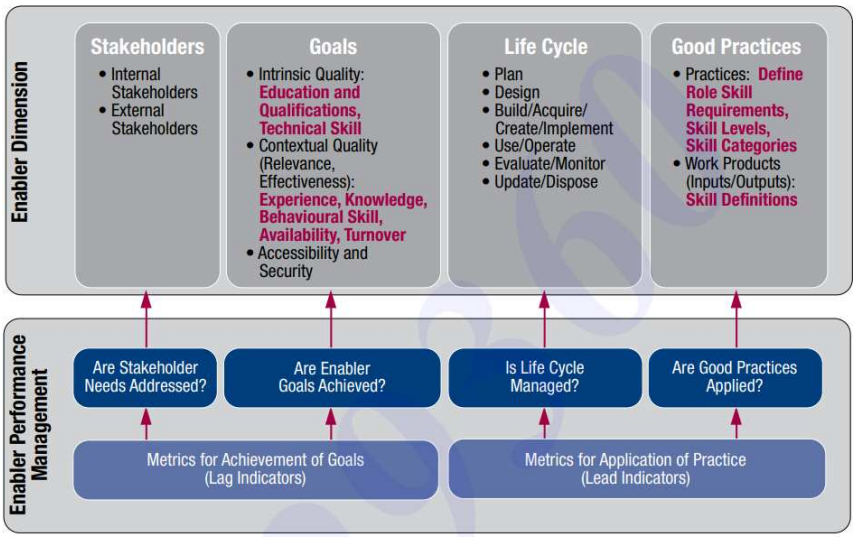


Figure 23: Enabler 7 of COBIT: people, skills and competencies (ISACA, 2012b).

Examples of good practices are definitions of the required skill levels for different stakeholders. These skills can be categorized and mapped. For each skill level within each skill category, there has to be a definition. These categories have to be in line with undertaken IT-related activities, such as information management. COBIT offers a generic overview of potential skill categories. These categories are specifically mapped for the COBIT process domains (ISACA, 2012b). This overview is as follows:

Process Domain	Examples of Skill Categories
Evaluate, Direct and Monitor (EDM)	• Governance of enterprise IT
Align, Plan and Organise (APO)	• IT policy formulation • IT strategy • Enterprise architecture • Innovation • Financial management • Portfolio management
Build, Acquire and Implement (BAI)	• Business analysis • Project management • Usability evaluation • Requirements definition and management • Programming • System ergonomics • Software decommissioning • Capacity management
Deliver, Service and Support (DSS)	• Availability management • Problem management • Service desk and incident management • Security administration • IT operations • Database administration
Monitor, Evaluate and Assess (MEA)	• Compliance review • Performance monitoring • Controls audit

Figure 24: COBIT's skill categories overview (ISACA, 2012b).

Appendix 12: NEN 7510's PDCA tasks

NEN 7510 describes different tasks to be done to set up the ISMS within healthcare organizations. This is based on ISO/IEC 27001 and ISO/IEC 27002. The steps are as follows:

Plan

1. Determining application areas and borders of the ISMS;
2. Integration of the ISMS in the organization's business operations;
3. Establishing the approach (risk appetite) for judging risks;
4. Identifying risks (identifying risk factors and organizational assets);
5. Analyzing and judging risks;
6. Picking the correct/corresponding risk treatment;
7. Picking managing targets and checks;
8. Preparing a statement of applicability;
9. Receiving approval of remaining risks for implementing the ISMS (NEN, 2017).

Do

1. Executing risk treatment;
2. Making the required assets available by the direction;
3. Realizing measures (planning actually necessary procedures);
4. Executing training and education (of employees);
5. Managing the execution of the ISMS;
6. Managing the measures of the ISMS;
7. Executing follow-up actions regarding information security incidents (NEN, 2017).

Check

1. Procedures for control and judgement;
2. Frequent estimation of the efficiency of the ISMS (efficiency and residual risk);
3. Judgement by the direction (NEN, 2017).

Act

1. Executing improvement measures (both corrective and preventative actions);
2. Communicating executed/implemented actions (NEN, 2017).

Appendix 13: Comparison between NIS2, NEN 7510 & other frameworks

NEN 7510 is compared with NIS2, as well as with other standards which are in scope of this research. There are four parts which NIS2 is built upon, which are 1) adopting cybersecurity strategies, 2) setting up cybersecurity risk measures & new reporting duties, 3) new rules and obligations regarding data sharing of cybersecurity information, and 4) supervisory and enforcement obligations as a member state of the EU. These four parts of NIS2 will be compared with the types of controls which are already present in the healthcare sector.

Each of the four parts of NIS2 is referred to as # (number). #1 stands for part one of NIS2, which is about adopting cybersecurity strategies, et cetera. An 'X' means that there is nothing in place for the specific framework. A 'C' is the abbreviation of the word chapter. The overview is presented in appendix 13.

The overview looks as follows:

Table 9: Frameworks useful for NIS2 overview compared

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
#1 – CSIRT task 1: monitoring	• X	• MEA01 (monitor, evaluate and assess performance and conformance) • MEA02 (Monitor, evaluate and assess the system of internal control) • MEA03 (Monitor, evaluate and assess compliance with external requirements)	• Monitoring enterprise risk management performance: 22 (Monitors substantial change) • Monitoring Enterprise Risk Management Performance: 23 (Monitors Enterprise Risk Management)	• All DE.CM (Detect, continuous monitoring) processes • All DE.AE (Detect, adverse event analysis) processes	• 4.3 Maintenance and monitoring of a risk action plan • 16.1 Security testing, surveillance and monitoring • 16.2 Monitoring of internal control framework

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
#1 – CSIRT task 2: analysis	• X	• APO01 (Manage the IT management framework)	• Risk in execution: 12 (identifies risk in execution) • Risk in execution: 13 (assesses severity of risk) • Risk in execution: 16 (assesses risk in execution)	• All DE.AE (Detect, adverse event analysis) processes	• 11.1 ICT Business impact analysis and ICT continuity plans
#1 – CSIRT task 3: Incident response	• X	• DSS02 (manage service requests and incidents)	• Risk information, communication, and reporting: 20 (communicates risk information)	• All RS.AN (Respond, incident analysis) processes	• 11.4 Restoration • 15.1 Security incident policy and definition • 15.2 Incident escalation • 19.1 Malicious software prevention, detection and correction
#1 – CSIRT task 4: Directing	• X	• DSS01 (Manage operations)	• Risk governance and culture: 4 (demonstrates commitment to integrity and ethics)	• All GV.PO (Govern, policy) processes	• 1.2 Information security policies and process management • 5.2 Management of information security

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
			• Risk governance and culture: 5 (enforces accountability)		and tasks of the information security function
#1 – CSIRT task 5: coordination	• X	• BAI04 (Manage availability and capacity) • BAI05 (Manage organizational change enablement	• Risk governance and culture: 1 (exercises board risk oversight) • Risk governance and culture: 2 (establishes governance and operating model) • Risk information, communication, and reporting: 20 (communicates risk information)	• All GV.RR (Govern, roles, responsibilities, and authorities) processes • All GV.PO (Govern, policy) processes • All GV.OV (Govern, oversight) processes	• 5.2 Management of information security and tasks of the information security function • 9.3 Employee awareness
#2 – Creating or updating policies on (one or more) risk analyses and information system security	• NEN 7510 part 1: C6.1 (measures to decrease risks and	• DSS04 (Manage continuity) • APO01 (Manage the IT management framework) • MEA02 (Monitor, evaluate and assess the system of internal control)	• All Risk, strategy and objective setting processes (7 – 11) • Risk information, communication, and reporting: 19	• All GV.PO(Govern, policy) processes	• 1.2 Information security policies and process management • 11.1 ICT Business impact analysis and ICT continuity plans

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
	utilizing opportunities) • NEN 7510 part 1: C8.2 (Risk assessment of information security) •		(leverages information systems)		• 15.1 Security incident policy and definition
#2 – Incident handling	• NEN 7510 part 2: C16 managing of information security incidents	• DSS02 (Manage service requests and incidents)	• All Risk in execution processes (12-17) • Risk information, communication, and reporting: 18 (uses relevant information) • Risk information, communication, and reporting: 20 (communicates risk information)	• All RS.X processes (MA (incident management), AN (incident Analysis), CO (incident response reporting and communication) and MI (incident mitigation))	• 11.4 Restoration • 15.1 Security incident policy and definition • 15.2 Incident escalation • 19.1 Malicious software prevention, detection and correction

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
			• Risk information, communication, and reporting: 21 (reports on risk, culture, and performance)		
#2 – Business continuity management	• NEN 7510 part 2: C12.3 (backup) • NEN 7510 part 2: C16.1 & C16.2 (reporting of information security events) • NEN 7510 part 2: C17 (information security	• DSS04 (manage continuity)	• All Monitoring enterprise risk management performance processes (22-23) • Risk in execution: 15 (identifies and selects risk responses) • Risk in execution: 17 (develops portfolio view)	• All DE.CM (Detect, continuous monitoring) processes • All RC.X processes (RP (incident recovery plan execution) and CO (incident recovery communication))	• 11.1 ICT Business impact analysis and ICT continuity plans • 11.2 Testing of the ICT continuity plan • 11.3 Uncompromisable back-up storage • 11.4 Restoration • 14.1 Third party and supplier services management • 14.2 Third party and supplier risk management • 21.1 Physical security measures

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
	aspects of business continuity management) • NEN 7510 part 2: C 12.1 & C12.2 (Change management)				
#2 – Security for the supply chain	• NEN 7510 part 2: C14.2 up until C14.7 (Outsources software development) • NEN 7510 part 2:	• APO13 (Manage security) • APO10 (Manage suppliers • APO08 (Manage relationships) • DSS05 (Manage security services)	• Risk, strategy, and objective-setting: 10 (considers risk while establishing business objectives) • Risk, strategy, and objective-setting: 11 (defines acceptable variation in performance)	• All GV.SC (Govern, cybersecurity supply chain risk management) processes	• 14.1 Third party and supplier services management • 14.2 Third party and supplier risk management

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
	C15.1 up until C15.3 (supply chain of information- and communication technology)		• Risk in execution: 17 (develops portfolio view)		
#2 – Security in (the) network and information systems acquisition, development and maintenance	• NEN 7510 part 2: C14 (acquisition, development and maintaining of information systems) • NEN 7510 part 2:	• APO13 (Manage security) • DSS02 (Manage service requests and incidents) • DSS05 (Manage security services) • BAI03 (Manage solutions identification and build) • BAI06 (manage changes)	• Risk, strategy, and objective-setting: 7 (considers risk and business context) • Risk in execution: 12 (identifies risk in execution) • Risk in execution: 16 (Assesses risk in execution) • Risk information, communication, and	• All GV.RR (Govern, roles, responsibilities, and authorities) processes • All GV.PO (Govern, policy) processes • All PR.AA (Protect, identity management, authentication, and access control) processes	• 1.2 Information security policies and process management • 2.1 Information security architecture • 2.2 Data classification scheme • 3.2 Technical standards • 5.2 Management of information security and tasks of the

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
	C12.6 (Managing of technical vulnerabilities)		reporting: 18 (uses relevant information) • Risk information, communication, and reporting: 19 (leverages information systems)	• All PR.PS (Protect, platform security) processes • All PR.IR (Protect, technology infrastructure resilience) processes	information security function • 6.1 Data and system ownership • 18.4 Network security • 19.1 Malicious software prevention, detection and correction • 19.2 Vulnerability management • 20.1 Protection of security technology • 21.1 Physical security measures •
#2 – Policies and procedures to assess the effectiveness of current cybersecurity risk management measures	• NEN 7510 part 1: C6.1 (measures to decrease risks and	• EDM03 (Ensure risk optimization) • MEA01 (Monitor, evaluate and assess performance and conformance)	• Risk governance and culture: 1 (exercises board risk oversight) • All Risk in execution processes (12-17)	• All GV.PO (Govern, policy) processes • All RS.AN (Respond, incident analysis) processes	• 4.2 Risk assessment • 10.2 Impact assessment, prioritization and authorization

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
	utilize opportunities)	• MEA02 (Monitor, evaluate and assess the system of internal control)		• All ID.IM (Identify, improvement) processes	• 16.1 Security testing, surveillance and monitoring • 18.3 Cryptography and cryptographic key management
#2 – Basic cyber hygiene setup and cybersecurity (awareness) trainings	• NEN 7510 part 2: entire document (not clear specifically which measures)	• BAI05 (Manage organizational change enablement) • BAI08 (Manage knowledge) • BAI07 (Manage change acceptance and transitioning) • BAI10 (Manage configuration) • EDM01 (Ensure governance framework setting and maintenance) • DSS04 (Manage continuity)	• Risk governance and culture: 2 (establishes governance and operating model) • Risk governance and culture: 3 (defines desired organizational behaviors) • Risk governance and culture: 5 (enforces accountability) • Risk governance and culture: 6 (attracts, develops, and retains talented individuals)	• All PR.AT (Protect, awareness and training) processes • All PR.AA (Protect, identity management, authentication, and access control) processes	• 1.1 Information security plan • 8.1 Personnel recruitment and retention • 8.2 Personnel competencies and culture • 9.1 Knowledge transfer to end users • 9.2 Knowledge transfer to operations and support staff • 9.3 Employee awareness

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
					• 16.3 Internal control at third parties
#2 – Policies and procedures regarding the use of cryptography & encryption	• NEN 7510 part 2: C10 (cryptography)	• EDM01 (Ensure governance framework setting and maintenance) • DSS04 (Manage continuity) • DSS05 (Manage security services) • APO13 (Manage security)	• Risk governance and culture: 3 (defines desired organizational behaviors) • Risk governance and culture: 5 (enforces accountability)	• All GV.PO (Govern, policy) processes • All PR.DS (Protect, data security) processes • All PR.PS (protect, platform security) processes • All PR.IR (Protect, technology infrastructure resilience) processes	• 1.2 Information security policies and process management • 3.1 Risks and opportunities of future trends and regulations • 4.2 Risk assessment • 18.3 Cryptography and cryptographic key management
#2 - Human resources security, access control policies and asset management	• NEN 7510 part 2: C7 (Secure/safe staff/employees) • NEN 7510 part 2: C8	• APO01 (Manage the IT management framework) • APO13 (Manage security) • BAI09 (Manage assets) • BAI10 (Manage configuration)	• Risk governance and culture: 4 (demonstrates commitment to integrity and ethics) • Risk governance and culture: 5 (enforces accountability)	• All GV.PO (Govern, policy) processes • All ID.AM (Identify, asset management) processes • All PR.AA (Protect, identity management,	• 2.2 Data classification scheme • 4.2 Risk assessment • 7.1 Segregation of duties • 8.5 Job change and termination

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
	(managing of the assets of the organization • NEN 7510 part 2: C9 (access security)	• MEA02 (Monitor, evaluate and assess the system of internal control)	• All Monitoring enterprise risk management performance processes (22-23)	authentication, and access control) processes	• 10.2 Impact assessment, prioritization and authorization • 13.1 Configuration repository and baseline • 17.1 Identity and access management • 18.4 network security • 19.2 Vulnerability management • 21.2 Physical access
#2 – The use of Multi-Factor Authentication (MFA) or continuous authentication solutions, Secured voice, video and text communications, secured emergency communication systems within the entity	• NEN 7510 part 2: C9.4.1 (limited access to information (MFA)) • NEN 7510 part 2: C9	• APO13 (Manage security) • BAI10 (Manage configuration) • MEA02 (Monitor, evaluate and assess the system of internal control) • APO01 (Manage the IT management framework)	• Risk governance and culture: 2 (establishes governance and operating model) • Risk governance and culture: 3 (defines desired organizational behaviors)	• All PR.AA (Protect, identity management, authentication, and access control) processes • All PR.PS (Protect, platform security) processes	• 17.1 Identity & access management • 17.2 User account management • 18.1 Infrastructure resource protection and availability • 18.5 Protection of sensitive data

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
	(access security) • NEN 7510 part 2: C15.1.3 (supply chain of information- and communication technology)		• Risk governance and culture: 5 (enforces accountability)	• All PR.IR (Protect, technology infrastructure resilience) processes	
#3 – Assessment of the severity of an incident	• X	• All Deliver, Service and Support processes (DSS01 - DSS06) • EDM05 (Ensure stakeholder transparency)	• All risk in execution processes (12-17)	• All RS.X processes (MA (Respond, incident management), AN (Respond, incident analysis), CO (Respond, incident response reporting and communication),	• 4.2 Risk assessment • 10.2 Impact assessment, prioritization and authorization • 18.2 Infrastructure maintenance • 19.3 Application maintenance

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
				MI (Respond, incident mitigation))	
#3 – Within 24 hours of an incident (depending of the severity), reporting an incident to the CSIRT or competent authorities	• X	• All Deliver, Service and Support processes (DSS01 – DSS06) • EDM05 (Ensure stakeholder transparency)	• All Risk information, communication, and reporting processes (18-21) • All monitoring enterprise risk management performance processes (22-23)	• All RC.X processes (RP (Recover, incident recovery plan execution) and CO (Recover, incident recovery communication))	• 4.1 ICT-Risk management framework • 5.1 Responsibility for risk, security, compliance and information security function • 5.2 Management of information security and tasks of the information security function • 12.1 Storage and retention arrangements • 15.1 Security incident policy and definition • 15.2 Incident escalation

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
					• 19.2 Vulnerability management
#3 - Within 72 hours, an incident notification, has to update the information referred to as reported in the incident report in the first 24 hours after the occurrence. Includes: initial assessment of the significance of the incident, including its severity and impact, and the indicators of compromise.	• X	• All Deliver, Service and Support processes (DSS01 - DSS06) • EDM05 (Ensure stakeholder transparency)	• All Risk information, communication, and reporting processes (18-21) • All monitoring enterprise risk management performance processes (22-23)	• All RC.X processes (RP (Recover, incident recovery plan execution) and CO (Recover, incident recovery communication))	• 4.1 ICT-Risk management framework • 5.1 Responsibility for risk, security, compliance and information security function • 5.2 Management of information security and tasks of the information security function • 12.1 Storage and retention arrangements • 15.1 Security incident policy and definition • 15.2 Incident escalation

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
					• 19.2 Vulnerability management
#3 - no later than one month after the incident, a detailed report has to be written. It includes a detailed description of the incident, including its severity and impact, the threat type or root cause which was likely to have triggered the incident, the ongoing as well as applied mitigation measures, and the cross-border impact of the incident.	• X	• All Deliver, Service and Support processes (DSS01 - DSS06) • EDM05 (Ensure stakeholder transparency)	• All Risk information, communication, and reporting processes (18-21) • All monitoring enterprise risk management performance processes (22-23)	• All RC.X processes (RP (Recover, incident recovery plan execution) and CO (Recover, incident recovery communication))	• 4.1 ICT-Risk management framework • 5.1 Responsibility for risk, security, compliance and information security function • 5.2 Management of information security and tasks of the information security function • 12.1 Storage and retention arrangements • 15.1 Security incident policy and definition • 15.2 Incident escalation

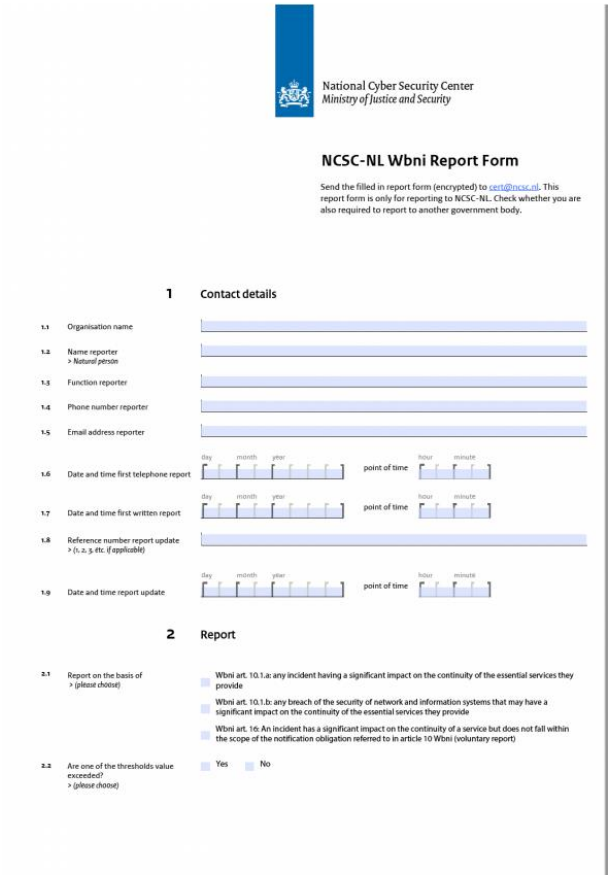
NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
					• 19.2 Vulnerability management
#3 – Deciding to voluntarily report an almost-incident	• X	• EDM04 (Ensure resource optimization) • EDM05 (Ensure stakeholder transparency)	• Risk, strategy, and objective-setting: 7 (considers risk and business context) • All Risk information, communication, and reporting processes (18-21) • All monitoring enterprise risk management performance processes (22-23)	• All RC.X processes (RP (Recover, incident recovery plan execution) and CO (Recover, incident recovery communication)) • All GV.RM (Govern, Risk Management Strategy) processes	• 4.1 ICT-Risk management framework • 5.1 Responsibility for risk, security, compliance and information security function • 5.2 Management of information security and tasks of the information security function • 12.1 Storage and retention arrangements • 15.1 Security incident policy and definition • 15.2 Incident escalation

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
					• 16.1 Security testing, surveillance and monitoring • 19.2 Vulnerability management
#4 – Determine if the organization is categorized as important or essential	• X	• DSS01 (Manage operations) • MEA03 (Monitor, evaluate and assess compliance with external requirements)	• Monitoring enterprise risk management performance: 23 (monitors enterprise risk management)	• All RS.CO (Respond, incident response reporting and communication) processes • All RC.X processes (RP (Recover, incident recovery plan execution) and CO (Recover, incident recovery communication)) •	X
#4 – Register (one-time) for the register where to report incidents towards	• X	• DSS01 (Manage operations) • MEA03 (Monitor, evaluate and assess compliance	• Risk governance and culture: 5 (enforces accountability)	• All RS.CO (Respond, incident response reporting and	X

NIS2 part	NEN 7510	COBIT 5	COSO	NIST	DNB
		with external requirements)	• Monitoring enterprise risk management performance: 23 (monitors enterprise risk management)	communication) processes • All RC.X processes (RP (Recover, incident recovery plan execution) and CO (Recover, incident recovery communication))	

Appendix 14: Wbni reporting form

Kamara & Van den Boom (2022) presented the Wbni form to report incidents. This can also be used for NIS2. The form looks as follows:



National Cyber Security Center
Ministry of Justice and Security

NCSC-NL Wbni Report Form

Send the filled in report form (encrypted) to cert@ncsc.nl. This report form is only for reporting to NCSC-NL. Check whether you are also required to report to another government body.

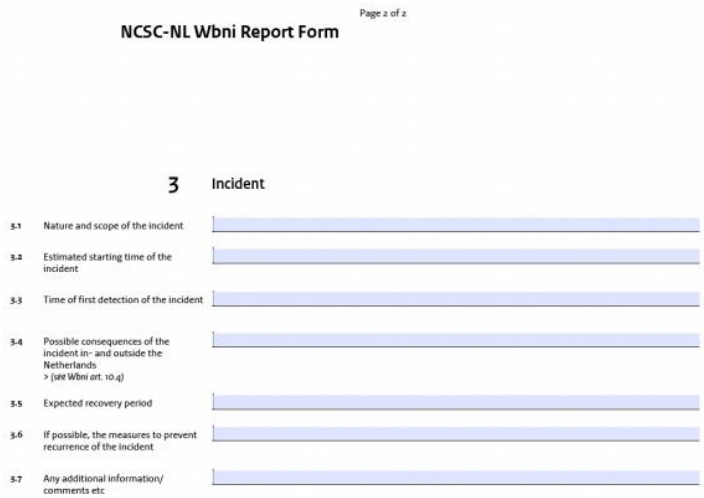
1 Contact details

1.1	Organisation name	
1.2	Name reporter > *Natural person*	
1.3	Function reporter	
1.4	Phone number reporter	
1.5	Email address reporter	
1.6	Date and time first telephone report	day month year point of time hour minute
1.7	Date and time first written report	day month year point of time hour minute
1.8	Reference number report update > (1, 2, 3, etc. if applicable)	
1.9	Date and time report update	day month year point of time hour minute

2 Report

2.1	Report on the basis of > (please choose)	Wbni art. 10.1.a: any incident having a significant impact on the continuity of the essential services they provide Wbni art. 10.1.b: any breach of the security of network and information systems that may have a significant impact on the continuity of the essential services they provide Wbni art. 16: An incident has a significant impact on the continuity of a service but does not fall within the scope of the notification obligation referred to in article 10 Wbni (voluntary report)
2.2	Are one of the thresholds value exceeded? > (please choose)	Yes No

Figure 25: Wbni incident reporting form part 1/2 (Kamara & Van Den Boom, 2022)



Page 2 of 2

NCSC-NL Wbni Report Form

3 Incident

3.1	Nature and scope of the incident	
3.2	Estimated starting time of the incident	
3.3	Time of first detection of the incident	
3.4	Possible consequences of the incident in- and outside the Netherlands > (see Wbni art. 10.4)	
3.5	Expected recovery period	
3.6	If possible, the measures to prevent recurrence of the incident	
3.7	Any additional information/ comments etc	

Figure 26: Wbni incident reporting form part 2/2 (Kamara & Van Den Boom, 2022)

Appendix 15: Risk times impact matrix & supply chain control measuring

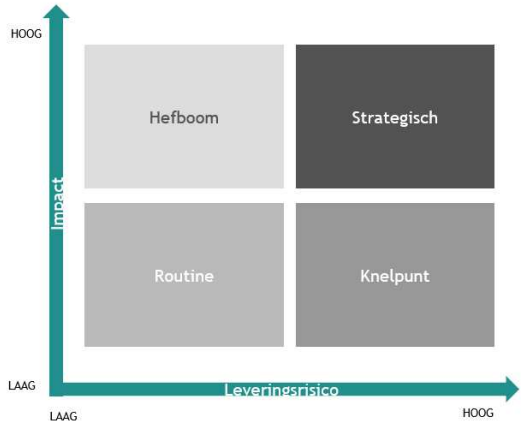


Figure 27: Determining the importance of the supply chain for NIS2 (BDO, 2024)

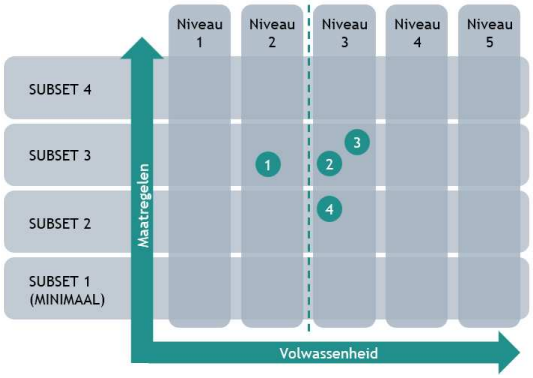


Figure 28: Determining the maturity for each NIS2 subset control (BDO, 2024)

Appendix 16: Standardized process & reporting form for significant incidents

The process for reporting incidents is based on NIS2's requirements. These are visualized in a process flow with the BPMN notation[13] as follows:

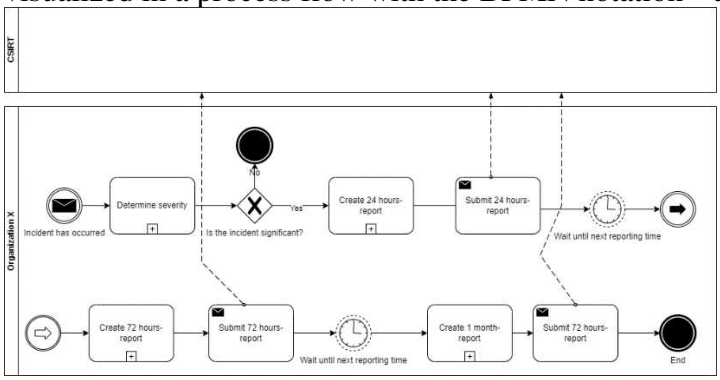


Figure 29: NIS2's reporting flow visualized

[13] BPMN stands for Business Process Model and Notation, and is a tool for visualizing process flows (Object Management Group, 2024).

Explanation on the process flow

The process flow starts with the event of an incident occurring. Then, the flow continues to processes which have to be executed. The "plus" signs on the bottom of the processes, such as the process 'Determine severity', shows that the process is actually a subprocess. There is a time interval in between the process steps. All subprocesses are explained below:

Subprocess: determine severity

Determining the severity of an occurred incident is the first step which needs to be done. An incident is considered significant when it:

- Leads to operational disruption within the organization;
- Leads to financial losses within the organization;
- Leads to having disruptions for others by causing considerable material or immaterial damage (Digital Trust Center, 2023; Overheid.nl, 2024).

If the answer to one of these questions is "yes", then the incident is considered significant, and three reports have to be created. These are presented in the next steps.

Subprocess: create 24 hours report

When an incident is considered significant, a few details on the incident have to be reported within the first 24 hours of the occurred event. Details which have to be reported are as follows:

- An early indication of the significance of the incident;
- An early indication of the severity of the impact of the incident;
- An indication of if the incident will have unlawful, malicious and/or harmful acts;
- An indication of if the incident will have an impact cross the border of the nation the organization is located in (European Parliament, 2022).

The consultation version of the Cbw states that an organization also has to report the information of the person who reported the incident. The CSIRT will also grant technical support if the organization requests this. A response from the CSIRT is also send within 24 hours of the first incident report received (Overheid.nl, 2024). When this report has been send, the next obligatory report is already on the way. Within 72 hours, the next report has to be created.

Subprocess: create 72 hours report

In the timespan between the first 24 hours and the first 72 hours of the occurred incident, a further analysis has to be conducted to write the findings in a report. These details include:

- Any updates regarding the already reported findings in the 24 hours report;
- An initial assessment of the incident, including:
    - The severity of the impact;
    - Indicators of the compromise (if applicable) (European Parliament, 2022).

The consultation version of the Cbw states that an organization also has to report all available information which allows the CSIRT and the authorized authority to determine any cross-border consequences (if applicable). The CSIRT may also ask for an intermediary report which has to update the CSIRT on the current status and relevant updates on the situation (Overheid.nl, 2024). When this report has been sent, the next obligatory report is on the way. This time, there is a bigger timespan in between the reports. Within 1 month, the next report has to be created.

Subprocess: create 1 month report

In the timespan between the first 72 hours and one month after of the occurred incident, a detailed analysis has to be conducted to write the findings in a report. This report needs to be sent to the corresponding CSIRT of the organization. These details include:

- A detailed description of the incident, including:
    - The final severity and impact of the incident;
    - The threat type or root cause which has likely triggered the incident;
    - The ongoing and already applied mitigation measures;
    - The cross-border impact of the incident (European Parliament, 2022).

The consultation version of the Cbw states that it is also possible that an incident has not been handled yet within one month. If this is the case, the organization has to hand in a final report based on the same requirements mentioned above within one month of the incident being handled.

Appendix 17: Email send to interview cybersecurity/health experts within BDO

The email was originally sent in Dutch. For convenience, it has also been translated into English.

Dutch

Beste [naam],

Mijn naam is Alwin van Welie. Momenteel schrijf ik mijn scriptie voor de studie Information Management aan de Tilburg Universiteit. Mijn thesis gaat over de NIS2 directive in de zorgsector, waarbij ik de NEN 7510 tegen NIS2 heb gelegd. Hierbij maak

ik een raamwerk, waarbij ik op basis van andere control frameworks zoals COBIT, COSO en NIST kijk welke maatregelen nog ingericht moeten worden.

Voor mijn onderzoek zou ik graag door middel van expertinterviews verifiëren of de inrichting van het framework klopt. Hiernaast zou ik graag meer informatie over huidige maatregelen in de zorg/cybersecurity sector verkrijgen.

Het interview zal 45 tot 60 minuten duren. Het interview zou ik graag afnemen in de in de periode tussen 7 en 14 juni. Dit kan zowel op kantoor Utrecht, online of op een ander BDO-kantoor in overleg. Gedurende deze periode kan ik op elk moment, maandag tot en met vrijdag. Als u beschikbaar bent, laat dan zeker uw voorkeurs datum en tijd weten. Dan zal ik een uitnodiging (via Outlook) creëren.

Ik hoor graag of u beschikbaar bent.

Met vriendelijke groet,
Alwin van Welie

English

Dear [name],

My name is Alwin van Welie. I am currently writing my thesis for the study Information Management at the Tilburg University. The subject of my thesis is the NIS2 directive in the healthcare sector, where I compared NEN 7510 to NIS2. I am creating a framework, where I use other frameworks such as COBIT, COSO and NIST to check which controls still have to be implemented.

For my research, I would like to verify my framework based on expert interviews. Next to this, I would like to receive more information on the currently taken controls/measures in the healthcare/cybersecurity sector.

The interview will take 45 to 60 minutes. I would like to conduct the interview in the period between the 7th and the 14th of June. This is possible physically at the office located in Utrecht, online or at another BDO-office in coordination. During this period, I am available all week, at the regular working hours. If you are available, please let me know your preference date and time. I will then send an invite (via Outlook).

I look forward to hear if you are available.

With kind regards,
Alwin van Welie

Appendix 18: ITIL 4's incident management steps

1. Incident identification;
    a. Ensures that incidents are identified before any negative business impacts may occur.
    b. Ensures that incidents are taken care of by the correct people.
2. Incident logging;
    a. Ensures that information is recorded fully and that sources are identified.
    b. Ensures that information is recorded in the right way to be used for the incident handling process.
    c. Ensures that a summary of the incident is presented.
3. Incident categorization;
    a. Ensures that the categorization of incident reports is done both efficiently and in a short timeframe.
4. Incident prioritization;
    a. Ensures that incoming incident reports are given priority based on severity and in a short timeframe.
    b. Ensures that the sufficient people work on solving the incident.
5. Initial diagnosis;
    a. Ensures that early diagnostic action is performed in time.
    b. Ensures that leaders and official instances receive priority on handling the incident.
    c. Ensures that early diagnostic measures are able to provide sufficient input for incident handling.
6. Incident escalation;
    a. Ensures that the escalation process is done in a short timeframe to meet the target SLA.
    b. Ensures that the escalation process is executed with considering the action taken already.
    c. Ensures that the selection of persons responsible for handling the incident is done.
7. Investigation and diagnosis;
    a. Ensures (through thorough and in-depth) investigation that the source of the incident is found.

   b. Ensures that both investigative and diagnostic activities are executed according to standards set in the SLA.
   c. Ensures that appropriate solutions are found for the incident.
8. Resolution and recovery;
   a. Ensures that solutions for the incident are tested and can be properly implemented.
9. Incident closure;
   a. Ensures that the closure of the incident is executed.
   b. Ensures that complaints of the incident reporter are accepted.
10. Incident management report;
   a. Ensures that daily recapitulation is executed.
   b. Ensures that monthly recapitulation is executed.
   c. Ensures that an incident response report is prepared as an evaluation for future action measures.
11. Incident management evaluation.
   a. Ensures that evaluations are executed on a monthly basis to improve the incident handling quality.
   b. Ensures that evaluation results from the incident are followed by each level of affected party (Palilingan & Batmetan, 2018).

Appendix 19: Controls/measures for the ITIL incident management steps

For each of the 11 steps that ITIL 4 presents for incident management, good practices and/or controls/mitigation measures are presented. These are based on the frameworks which have been looked at in detail in chapter 5 (current framework analysis).

Step 1: Incident identification

Good practice based on the DNB: classify incidents based on their impact, based on the following criteria:

- The number of people/organizations involved and the relevance of their affected assets;
- The outage time that the incident was responsible for;
- The geographical distribution of the incident, if the incident reaches further than just one region the organization is in;
- The data loss which the IT-related incident brings with itself, such as loss within the CIA-triad;
- The critical character of involved service organizations;
- The economic impact, with the emphasis on the direct and indirect costs and losses, both in relative and absolute sense (De Nederlandsche Bank, 2023).

Next to this, DNB has created good practices to make sure that the incident is handled sufficiently and by the correct people:

- The security officer of the organization determines on a daily basis the registered security incidents' impact;
- The organization and the service providers work together proactively at detecting and reacting to cybersecurity incidents. The organization has a Security Operations Center (SOC) or Cyber Defense Center in place, or alternatively, the organization makes use of a commercial external SOC.
- A Security Information and Event Management (SIEM) solution is implemented to (based on logging) check and react on divergent patterns (De Nederlandsche Bank, 2023).

Step 2: Incident logging

To ensure that incident information is recorded in a complete form in the right way and that sources are identified, the following good practice is presented by DNB:

- Based on (high impact) incidents, a root cause analysis (RCA) is conducted to determine on which level employees have contributed to the incident. The RCA looks into sloppiness, dissatisfaction of employees, and cultural aspects.
- Incident information is recorded into the SIEM or a similar system (De Nederlandsche Bank, 2023).

COBIT presents the following measures:

- Events have to be logged by using infrastructure monitoring tools, and the level of information to be recorded has to be based on the risk and performance (change) of the organization;
- Event logs have to be produced and retained for an appropriate timeframe to assist in future investigations (ISACA, 2012a).

NIST CSF references to the FIPS 200[14] minimum security requirement specifications:

- Identification of system users, processes initiated by a specific user, or devices and verification which are allowed to access the organization's ICT systems.

NIST CSF also states the following:

- "*Organizations must establish an operational incident handling capability for organizational ISs that includes adequate preparation, detection, analysis, containment, recovery, and user response activities*" (Kohnke et al., p. 275).

Step 3: Incident categorization

[14] FIPS 200 offers minimum security requirements for Federal Information and Information Systems (NIST, 2006).

Step 1 already offered some ways how to categorize incidents, based on DNB. COBIT offers additional notes on incident categorization:

- Incidents have to be categorized and actual exposures have to be compared against tolerance thresholds. The business impact has to be communicated to decision makers as part of reporting. The risk profile should also be updated (ISACA, 2012a).

Step 4: Incident prioritization

To ensure that the correct people are working on solving the incident as well as prioritizing different incidents based on severity, the COSO ERM offers the following:

- Risks that impact the achievement of strategy and business objectives are identified and assessed. They are prioritized based on severity, in the context of the risk appetite that the organization has defined. The organization then selects responses and takes a portfolio view of the amount of risk it has assumed (Committee of Sponsoring Organizations of the Treadway Commission, 2016).

Next to this, the classification good practice (see step 1) by the DNB also offers ways how to prioritize incidents. COBIT states the following on incident prioritization:

- Priority has to be defined through levels of consultation with the business to ensure that identifying incidents and RCA are executed in a timely manner based on the agreed-on Service Level Agreements (SLAs). The priority has to be based on business impact and urgency (ISACA, 2012a).

Finally, COBIT offers a way prioritize which person or groups of people work on solving an incident:

- Appropriate support groups have to be created (or already in place) to assist with problem identification, RCA, and working on a solution regarding the incident. The support groups have to be determined based on pre-defined categories, such as network, software, applications, support software, and hardware (ISACA, 2012a).

Step 5: Initial diagnosis

To make sure that diagnostic action is performed in time, that the measures are able to provide sufficient input for the handling of the incident and that leaders and official instances receive priority on handling the incident, DNB has come up with the SIEM as mentioned in step 2. Next to this, COBIT offers the following:

- Reports have to be produced to communicate the progress in resolving problems, as well as to monitor the continuing impact of the incidents which are not solved. The status of the problem-handling process for the ongoing

incidents has to be monitored throughout its life cycle. This includes input from change and configuration management (ISACA, 2012a).

Step 6: Incident escalation

In step 4, COBIT already presented measures to meet the set SLAs regarding incidents. In step 5, COBIT presented measures to make sure the incident escalation process is monitored while it is being solved. To ensure that the incident escalation process is executed with the consideration of the already taken action, it is important that previous incidents have been learned from. This can be both from inside the information as from peer organizations. This knowledge needs to be used in the incident escalation process. The DNB offers the following:

- The organization analyses and learns from incidents that have taken place at peers or other comparable organizations;
- The organization's management evaluates on a yearly basis, as well as with big IT-related incidents, the results of the current IT framework in place. Risks and actual developments are taken into account (De Nederlandsche Bank, 2023).

Step 7: Investigation and diagnosis

To make sure that the source of the incident is found, and that appropriate solutions are found for the incident, COBIT states the following:

- Incidents have to be identified and classified through the correlation of incident reports, error logs, and other problem identification sources. Priority levels and categorization has to be determined to address problems in time based on service definition and business risk.
- All incidents have to be formally handled with access to all relevant information, including data from the change management system and IT asset/configuration, as well as incident details.
- As soon as the RCAs of the incidents are found, known-error records have to be created as well as an appropriate workaround.
- Via change management, the identification, evaluation, prioritization, and processing of solutions to known errors needs to be based on a cost-benefit business case and based on the impact and urgency of the change (ISACA, 2012a).

Step 8: Resolution and recovery

To ensure that solutions for the incidents are properly implemented and that they can be tested, certain controls need to be in place. COBIT offers the following:

- After solutions or workarounds for incidents have been found, the problem records have to be closed.
- The service desk needs to be informed to schedule the problem closure (e.g. to create the schedule to solve the incident via change management).
- The solution or workaround needs to be reviewed and monitored over time to test if it still works sufficiently.
- The learned lessons and new knowledge needs to be incorporated into a service review meeting (ISACA, 2012a).

To ensure that the solutions are tested over time, DNB states the following:

- The organization executes (and lets this also be done by an external party) different information security tests, such as penetration tests (pentests) aimed towards all aspects of cybersecurity.
    - External parties which perform pentests have the sufficient knowledge necessary, as well as enough experience, certifications, and references.
    - The organization changes external parties which perform pentests frequently.
- The organization involves her critical or important service providers in the security tests.
- The organization executes several types of tests, such as a system test, acceptation test, regression test, and integration test to measure the effectiveness of information security measures in changed applications and infrastructure.
- Information security and cybersecurity are explicitly taken into account while testing changes. This can be done by executing security & vulnerability scanning and source code reviews (De Nederlandsche Bank, 2023).

Step 9: Incident closure

Step 8 already presented ways how to handle the closure of incidents. To ensure that complaints of the reporter of the incidents are accepted, it is important to take these people into the change process of finding solutions. This was already presented in steps 7 and 8.

Step 10: Incident management report

To ensure that an incident response report is created, the information obligatory to report according to NIS2 needs to be taken into account (see appendix 16). Next to this, step 6 already presented ways how to learn from past incidents.

Step 11: Incident management evaluation

To improve the incident handling process, evaluations of the current process should be done on a monthly basis. The results of the solution and current status regarding the incident also has to be reported to stakeholders (affected parties). Briefing other parties can be done as follows according to COBIT:

- Based on control exceptions, it needs to be decided which information is communicated to affected parties.
- Verifying with affected parties that the service request (change) has been successfully fulfilled or if the incident has been satisfactorily resolved (ISACA, 2012a).

Appendix 20: Interview questions: framework verification

The questions for the interviews to verify the framework are based on the six identified gaps which are presented in the framework. Based on the expertise of the interviewees within BDO, the interview protocols are also slightly different. They are as follows:

Interview protocol: healthcare professionals (Dutch)

Introductie

1. Hoe kan je een goede control opstellen?
2. Zijn er binnen BDO audits uitgevoerd voor de Wbni zover u weet?

Vragen over huidige werking zorgsector

3. Hoe gaan zorgorganisaties momenteel om met de toeleveranciers van systemen? Zowel binnen de zorgsector en met organisaties buiten de sector?
4. Is NEN 7510 in elke zorgorganisatie waar u een opdracht voor heeft gedaan de standaard?
    a. Zo nee, welke alternatieven heeft u gezien?
5. Hebben alle zorgorganisaties waar u een opdracht voor heeft gedaan minstens één verantwoordelijk persoon voor de IT binnen de organisatie?
    a. Wordt dit vaak uitbesteed? Zo ja, wat wordt vooral uitbesteed?
6. Van welke maatregelen heeft u gezien of vernomen dat zorgorganisaties al hebben of nog gaan implementeren?
7. Ziet u dat organisaties self-assessments uitvoeren om hun volwassenheid op het gebied van cybersecurity te meten en te verbeteren?
8. Waar ziet u dat er vooral uitdagingen en verbeteringen mogelijk zijn op het gebied van informatiebeveiliging?

Vragen over huidige frameworks gebruikt in praktijk

9. Hebben zorgorganisaties waar u een opdracht voor heeft gedaan een protocol (gestandaardiseerd of niet) voor het vaststellen van cybersecurity incidenten?

    a. Hebben deze organisaties ook een reactieplan voor gebeurde incidenten?

Vragen over het gemaakte framework (gaps benoemen/framework laten zien)

10. Momenteel wordt NEN 7510 als uitgangspunt voor de gehele zorgsector gebruikt voor het framework. Kan NEN 7510 volgens u als uitgangspunt worden genomen voor alle soorten organisaties binnen de zorgsector om voor te bereiden om NIS2 compliant te zijn?
11. NIS2 eist dat ook management trainingen volgt om risico's wat betreft NIS2 te kunnen identificeren. Denkt u dat een gezamenlijke training (met meerdere soorten medewerkers in de organisatie) of een aparte training beter zal werken?
    a. Moet de training anders opgezet worden mits management aparte trainingen krijgt?
12. Is het framework praktisch toepasbaar?
13. Welke risico's of elementen worden niet afgedekt met dit framework?

Afronding

14. Heeft u nog verdere vragen of opmerkingen wat betreft dit onderzoek?

Interview protocol: healthcare professionals (Translated)

Introduction

1. How can you create a sufficient control?
2. Have there been any audits regarding the Wbni within BDO as far as you know?

Questions about the working of the current healthcare sector

3. How are healthcare organizations currently dealing with suppliers of their systems? Both within the healthcare sector and with organizations outside of the healthcare sector?
4. Has NEN 7510 been the standard for all types of healthcare organizations that you have worked for?
    a. If not, which alternatives have you seen?
5. Do all healthcare organizations that you have worked for have at least one responsible person for IT within the organization?
    a. Is this something which is often outsourced? If this is the case, what is often outsourced?
6. Which measures have you seen or know that healthcare organizations are going to implement?
7. Do you see in practice that healthcare organizations execute self-assessments to measure the maturity of their cybersecurity in order to improve it?

8. Where do you see that challenges and improvements are possible in the information security domain?

Questions about current frameworks in practice

9. Do healthcare organizations which you have worked for have a protocol for (either standardized or not) for establishing cybersecurity incidents?
    a. Do these organizations also have a response plan for occurred incidents?

Questions about the created framework

10. Currently, NEN 7510 is taken as a starting point for the entire healthcare sector for the created framework. Do you think that NEN 7510 can be taken as a starting point for all healthcare organizations to prepare to become NIS2 compliant?
11. NIS2 mandates that management follows trainings to be able to identify risks regarding NIS2. Do you think that a simultaneous training (with several types of employees within an organization, such as juniors, managers and management) should have a training together or should this be separated?
    a. Do you think that the training should be different if management were to get different trainings?
12. Is the framework applicable in practice?
13. Which risks or elements are not covered by the framework?

Ending

14. Do you have any additional questions or remarks regarding the research?

Interview protocol: cybersecurity professionals (Dutch)

Introductie

1. Hoe kan je een goede control opstellen?
2. Zijn er binnen BDO audits uitgevoerd voor de Wbni zover u weet?

Vragen over huidige werking zorgsector

3. Hoe gaan zorgorganisaties momenteel om met de toeleveranciers van systemen? Zowel binnen de zorgsector en met organisaties buiten de sector?
4. Hebben alle zorgorganisaties waar u een opdracht voor heeft gedaan minstens één verantwoordelijk persoon voor de IT binnen de organisatie?
    a. Wordt dit vaak uitbesteed? Zo ja, wat wordt vooral uitbesteed?
5. Van welke maatregelen heeft u gezien of vernomen dat zorgorganisaties al hebben of nog gaan implementeren?
6. Ziet u dat organisaties self-assessments uitvoeren om hun volwassenheid op het gebied van cybersecurity te meten en te verbeteren?

7. Waar ziet u dat er vooral uitdagingen en verbeteringen mogelijk zijn op het gebied van informatiebeveiliging?

Vragen over huidige frameworks gebruikt in praktijk

8. Hebben zorgorganisaties waar u een opdracht voor heeft gedaan een protocol (gestandaardiseerd of niet) voor het vaststellen van cybersecurity incidenten?
    a. Hebben deze organisaties ook een reactieplan voor gebeurde incidenten?

Vragen over het gemaakte framework (gaps benoemen/framework laten zien)

9. NIS2 eist dat ook management trainingen volgt om risico's wat betreft NIS2 te kunnen identificeren. Denkt u dat een gezamenlijke training (met meerdere soorten medewerkers in de organisatie) of een aparte training beter zal werken?
    a. Moet de training anders opgezet worden mits management aparte trainingen krijgt?
10. Is het framework praktisch toepasbaar?
11. Welke risico's of elementen worden niet afgedekt met dit framework?

Afronding

12. Heeft u nog verdere vragen of opmerkingen wat betreft dit onderzoek?

Interview protocol: cybersecurity professionals (translated)

Introduction

1. How can you create a sufficient control?
2. Have there been any audits regarding the Wbni within BDO as far as you know?

Questions about the working of the current healthcare sector

3. How are healthcare organizations currently dealing with suppliers of their systems? Both within the healthcare sector and with organizations outside of the healthcare sector?
4. Do all healthcare organizations that you have worked for have at least one responsible person for IT within the organization?
    a. Is this something which is often outsourced? If this is the case, what is often outsourced?
5. Which measures have you seen or know that healthcare organizations are going to implement?
6. Do you see in practice that healthcare organizations execute self-assessments to measure the maturity of their cybersecurity in order to improve it?
7. Where do you see that challenges and improvements are possible in the information security domain?

Questions about current frameworks in practice

8. Do healthcare organizations which you have worked for have a protocol for (either standardized or not) for establishing cybersecurity incidents?
    a. Do these organizations also have a response plan for occurred incidents?

Questions about the created framework

9. NIS2 mandates that management follows trainings to be able to identify risks regarding NIS2. Do you think that a simultaneous training (with several types of employees within an organization, such as juniors, managers and management) should have a training together or should this be separated?
    a. Do you think that the training should be different if management were to get different trainings?
10. Is the framework applicable in practice?
11. Which risks or elements are not covered by the framework?

Ending

12. Do you have any additional questions or remarks regarding the research?

Appendix 21: Color coding interview transcripts

To be able to properly derive information from the transcripts of the interviews with the experts within BDO, color coding has been used. For the different identified gaps (6) as presented in chapter 6, as well as generic information which is useful for improving the research. The interviews are only available on request. The color coding looks as follows:

Gap 1: Incident management (GREEN)

Gap 2: Standardized reporting (YELLOW)

Gap 3: Contact with the CSIRT (TURQUISE)

Gap 4: Standardized impact assessment (PINK)

Gap 5: Mandatory cybersecurity risk management education for management (DARK RED)

Gap 6: Supply chain cybersecurity assessment (GRAY)

Generic information (RED)

Appendix 22: List of interviewed experts

Expert	Function	Department	Experience	Expertise	Interview aim
1	Senior manager	IT Risk Assurance	15 years	Healthcare	Verification
2	Senior manager	IT Risk Assurance	10 years	Healthcare	Verification

3	Senior manager	Cybersecurity	12 years	Cybersecurity	Verification
4	Cyber security consultant	Cybersecurity	4 years	Healthcare & cybersecurity	Verification
5	Junior manager	IT Risk Assurance	6.5 years	Cybersecurity	Verification
6	Senior manager	Cybersecurity	15 years	Healthcare & cybersecurity	Verification
7	Senior manager	IT Risk Assurance	8 years	Healthcare & privacy	Verification
8	Partner	IT Risk Assurance	12 years	Cybersecurity	Verification
9	Junior manager	IT Risk Assurance	5 years	Healthcare	Verification & validation (2 interviews)
10	Senior manager	IT Risk Assurance	9 years	Government	Verification
11	Junior manager	IT Risk Assurance	5.5 years	Healthcare	Validation

Table 10: List of interviews done with experts for framework verification and evaluation

Appendix 23: Pilot interviews, survey and email

This appendix presents the conducted pilot interviews, as well as the emails send to set up the pilot interviews and a created survey prior to the pilot interviews. The acquisition of two IT professionals within BDO went via a junior manager within BDO. Both IT professionals have the same level of experience in the same department. I emailed them two times, one time regarding the survey and once regarding the scheduling of the meeting for the interview.

Interview survey & questionnaire (translated into English from Dutch)

1. When did you first hear about NIS2?
    - Option 1: 2022 or earlier;
    - Option 2: 2023;
    - Option 3: 2024.
2. What percentage of your colleagues at the IT audit department is familiar with NIS2 according to your estimation?
    - Option 1: 0-20%;
    - Option 2: 20-40%;

   - Option 3: 40-60%;
   - Option 4: 60-80%;
   - Option 5: 80-100%.
3. What percentage of the current organizations where you currently work for, or have worked for in the past, is according to your estimation familiar with NIS2?
   - Option 1: 0-20%;
   - Option 2: 20-40%;
   - Option 3: 40-60%;
   - Option 4: 60-80%;
   - Option 5: 80-100%.
4. On a scale of 1-5, how familiar are you with the (potential) consequences and/or sanctions when organizations don't comply with the NIS2 directive? 1 means not familiar, 5 means completely familiar.
   - 1;
   - 2;
   - 3;
   - 4;
   - 5.
5. COBIT 5 describes '5 principles'. Which of the five do you think is/are the most important for a NIS2 compliance framework? (Several answers are possible, this will be discussed in the interview)
   - Meeting stakeholder needs;
   - Covering the enterprise end to end;
   - Applying a single integrated framework;
   - Enabling a holistic approach;
   - Separating governance from management.
6. ITIL 4 describes 7 'leading principles'. Which of the seven do you think is/are the most important for a NIS2 compliance framework? (Several answers are possible, this will be discussed in the interview)
   - Focus on value;
   - Start where you are;
   - Progress iteratively with feedback;
   - Collaborate and promote visibility;
   - Think and work holistically;
   - Keep it simple and practical;
   - Optimize and automate.

7. Which (elements of) frameworks, theories and/or other maturity models should, according to you, next to COBIT 5 and ITIL 4 be taken into consideration in the creation of a NIS2 framework?
    - ISO27001/NEN7510 (NEN 7510 for the healthcare sector);
    - ISO38500 (for governance);
    - The CMMI maturity model;
    - Six Sigma/elements of Lean;
    - The Balanced Scorecard;
    - Other: further details to be discussed in the interview.

The pilot interviews were created based on the outcomes of the *individuals*. The prompt for one of them is as follows (translated into English from Dutch and anonymized):

1. First of all, welcome [name]! Thanks for being here to speak about NIS2. What is your background within BDO and expertise within BDO Digital? What are your interests?
2. You mentioned that you are [level of familiarity] with the consequences/sanctions of NIS2 when organizations do not comply. What is your general knowledge regarding NIS2?
3. You mentioned that you heard of NIS2 in the year [year] for the first time. How did you get to know NIS2?
4. According to your estimation, [level of estimation] is (only) familiar with NIS2 on the [department name]. Could you elaborate a bit on this?
5. [Level of organizations] that you currently work for or have worked for in the past, is (only) familiar with NIS2 according to your estimation. Could you elaborate on what types of organizations this is the case?
6. COBIT describes five principles. You mentioned that [chosen answer(s)] was/were the most important elements for the creation of a new NIS2-compliance framework. How would you see these/this element(s) being incorporated into the framework?
7. ITIL describes seven leading principles. You mentioned that [chosen answer(s)] was/were the most important element(s) for the creation of a new NIS2-compliance framework. How would you see these/this element(s) being incorporated into the framework?
8. Next to COBIT and ITIL I will also look at other maturity models/framework which may (partly) suit within a new NIS2-framework. You mentioned that [chosen choice(s)] is/are good addition(s) to the new framework. Which

element(s) of the [chosen choice(s)] do you think will suit and how do you see this incorporated?

9. [Optional question] You mentioned that another, not specified framework/maturity model or theory could also be useful for the creation of a new NIS2-framework. Which model is this and how do you think it can contribute to a new NIS2-framework?
10. Chances are that NIS2 will be audited by a specially dedicated party/authority. What role do you expect BDO to fulfill if this is the case?
11. When a NIS2-compliance framework is created, elements such as assessing the maturity and recommending things to improve will become visual. How do you see BDO helping other organizations with this framework in the future?
12. Are there any questions or concerns which I may have missed according to you?
13. Would you like to stay involved in the thesis progress, and yes, how can I reach you?

Invitation emails

Survey email (translated into English from Dutch):

Good morning [name],

My name is Alwin van Welie! I'm currently a thesis intern at the [department name] of BDO. You have probably already read my introductory text on the intranet. I'm studying the double degree ITEM program, which stands for Information Technology for Enterprise Management. This is a master's program with Information Management master as a basis. The program started in Tilburg, and I'm currently in Turku (Finland). Because of this, I'm currently working in Finland on my thesis. For the thesis itself, I will develop a framework 'how to comply' with the soon-to-be implemented NIS2 cybersecurity legislation. I will conduct interviews for this, to get to know how much knowledge there already is within BDO, as well as to validate which things are important for a NIS2/framework based on the literature review.

I´m currently working on the literature review to determine which elements are important for NIS2. For this part I would like to interview you, where your perceptions regarding NIS2 will come forward. Before this interview is held, I will send you a short survey. This way, we can go into detail on certain things based on your survey response.

I will send the survey on [date] to you. Finalizing the survey will not take longer than a few minutes.

Do you have to for the interview in [week number]? This way, I have time to analyze your survey response and to prepare the interview. The time does not matter for me, but earlier in the week would suit me better. This is because of the progression of the thesis. The used medium for the interview doesn't matter to me.

Thanks in advance! I look forward to speaking with you.

With kind regards,
Alwin van Welie

Interview email (translated into English from Dutch):

Good morning [name],

At the end of this email I put a link to Google Meet for the interview for next week. If Teams would suit you better, could you create a meeting for it for me? This way, I also see your time preference.

I have not added a time yet for the meeting, since we still have to decide on it. Below I have proposed a few dates and times when we could meet:
[proposed dates and times to meet].

The interview will take an hour at maximum. The survey will be sent in another email today.

[link to Google Meet]
With kind regards,
Alwin van Welie

Appendix 24: Validation interview questions

For the validation interviews, I looked at the second iteration of the framework with a 'Cyber in the Audit' check together with two healthcare experts within BDO. The questions asked are as follows (translated into English from Dutch):

General questions

1. Can we take any healthcare organization to look at except a hospital? (interview 1)
2. Can we take a hospital to look at? (interview 2)

Verification questions

3. Are the controls' frequencies similar to real scenarios?
4. Are the controls of the framework applicable in practice?

Finalization questions

5. Do you have any questions or remarks regarding the research?

Appendix 25: Snippet of the framework with maturity levels selected

It is possible to select different maturity levels in the framework by selecting the related maturity level for a certain healthcare organization. This is done by copying the framework into Excel into a table, where the maturity levels are selectable. This Excel document is made for BDO. The snippet below shows maturity levels 3 and 4 selected.

Explanation	Topic (T)	Control (C)	Maturity level
A standardized incident reporting procedure needs to be created. Incidents need to be assessed so that these can be reported sufficiently to the CSIRT.	G1T2: Monitor potential threats.	G1T2C2: Logging of incidents is done in a SIEM (Security Information and Event Management) solution. This is evaluated on a daily basis by the security officer.	Level 3
A standardized incident reporting procedure needs to be created. Incidents need to be assessed so that these can be reported sufficiently to the CSIRT.	G1T2: Monitor potential threats.	G1T2C3: The security officer sets up a Security Operations Center (SOC) or Cyber Defense Center, or alternatively, the organization makes use of a commercial external SOC. The input of the SOC or Cyber Defense Center is checked and evaluated monthly.	Level 3
A standardized incident reporting procedure needs to be created. Incidents need to be assessed so that these can be reported sufficiently to the CSIRT.	G1T5: Audit/test the current IT incident framework on a yearly basis.	G1T5C2: An external, independent auditor audits the current IT incident framework on a yearly basis. The security officer is responsible for contacting the correct organisations/people for this.	Level 4
Management needs to develop competencies to assess be able to identify the risks regarding the security of network- and information systems, to judge the current risk control measures, and to judge implications of risks and risk control measures. This needs to be based on participation in tests and exercises.	G5T3: Trainings, tests and exercises need to be regularly conducted.	G5T3C2: The security officer sets up at least one training/exercise/test semi-annually for management. This may also be outsourced to instances with more experience regarding cybersecurity risk education for management specifically.	Level 3
The entire supply chain of information sending and receiving with external organisations needs to be assessed to improve cybersecurity in the entire supply chain.	G6T1: A list of all external organisations which either sends or receives information of the organisation needs to be documented.	G6T1C3: The procurement manager, together with the security officer, identifies all external partner organisations which are in the lever and bottleneck quadrants ('Hefboom': low supply risk and high impact risk and 'knelpunt': high supply risk and low impact if this partner cannot deliver information/their services) based on appendix 15.	Level 3

Figure 30: Snippet of the framework with maturity levels 3 and 4 selected

Appendix 26: DNB's maturity levels

Maturity level 1

The first level is named 'initial'. This level is reached when an organization has (partly) defined the measure, but it is executed in an inconsistent manner. There is a great level of dependence on individuals with the execution of the control measure. Criteria to clarify this level is as follows:

- No or limited control measures are implemented;
- The control measure is executed in an ad-hoc manner;
- The control measure is not documented;
- The manner in which the control measure is executed is dependent on an individual and is not standardized;
- The tasks and responsibilities including essential segregation of duties are described for the control, but is not executed conform the described description;
- Audits on the working of the control take place on an incidental basis;
- The effect of the control measure is not judged (De Nederlandsche Bank, 2023).

Maturity level 2

The second level is named ‘repeated but informal’. This level is reached when the control measure is present and is executed on a consistent and structured, but informal manner. Criteria to clarify this level is as follows:

- The creation and existence of the measure can be proven in only a limited way;
- The control measure is only partly defined, partly defined in a written way and partly embedded into the organization itself;
- The tasks and responsibilities including essential segregation of duties are described for the control measure and are executed in practice;
- The effect of the control cannot be proved and/or is not recorded;
- The working of the control measure is audited and recorded less than six months periodically, which means that the effectivity of the measure cannot be proven over a timespan of six months (De Nederlandsche Bank, 2023).

Maturity level 3

The third level is named ‘defined’. This level is reached when the setup of the control measure is documented and executed in a formal and structured manner. The required effectivity of the control measure is provable and is audited. Where necessary, the control measure is improved. Criteria to clarify this level is as follows:

- The setup, existence and effective working of the control measure are provable;
- The control measure is defined based on a risk assessment;
- The control measure is determined, recorded in a written manner (documented) and embedded into the organization;
- The tasks and responsibilities including essential segregation of duties are implemented based on a written determination and audited as well as evaluated based on their effectivity;
- The effective working of the control measure is audited at least each six months in a risk-based manner which is provable and documented;
- Management is informed about the execution of the control measure (De Nederlandsche Bank, 2023).

Maturity level 4

The fourth level is named ‘effective and measurable based on control measures’. This level is reached when all criteria for maturity level 3 are met, as well as some other requirements. These are that next to the effectivity of individual control measures, periodically also the effectivity of the coherence of the control measures is evaluated. This evaluation is reported and presented to the management of an organization. Criteria to clarify this level is as follows:

- The evaluation of the control measure takes place in the context of the coherence between all information security control measures;

- This evaluation of coherence between all control measures is documented;
- The tasks and responsibilities for the evaluation is formalized;
- The frequency on which is evaluated is based on the risk profile of the organization and takes place at least once each year;
- At the periodical assessment of the effective working of the control KCI's (metrics) are used and operational incidents are taken into account, and a peer-based benchmark takes place;
- The outcome of the evaluation is reported to the management (De Nederlandsche Bank, 2023).

Maturity level 5

The fifth level is named 'continuously improving and control measures are future focused'. This level is reached when all criteria for maturity level 4 are met, as well as some other requirements. These are that improvement regarding the coherence of control measures is constantly searched for by taking future scenarios into consideration. External data is used for benchmarking. Employees are proactively involved in the future aimed improvement of the effectivity of the coherence of the information security control measures. Criteria to clarify this level is as follows:

- The control measure is updated continuously. Evaluation is based on the future, and the peer-based benchmarking is taken into account within the evaluation;
- While designing of the control measure, results from self-assessments, gap- and root cause analyses are taken into account;
- The taken control measures are benchmarked based on external data and are considered as a 'best practice' compared to other organizations;
- The assessment of the effective working of the control measure is done based on KCI's (metrics);
- Employees are proven proactively involved at all times within improving the control measures (De Nederlandsche Bank, 2023).

Appendix 27: Elaboration on creation of framework controls

In order to create controls for the six gaps, controls and measures presented in other frameworks which were in scope of the research were used. For each of the frameworks studied, connections to NIS2's requirements are made. For these connections, examples and explanations for certain controls are given which have led to the first iteration of controls for the NIS2 framework. This appendix elaborates on how these controls have been created.

Gap 1: Incident management

COSO states that training should be implemented in the business continuity plan (BCP). All members of an organization should be aware of the procedures of the BCP (Moeller, 2011). However, since experts from the interviews have told that in practice this information is not presented in a BCP but rather in a policy regarding information security, it has been chosen to use this in the framework.

COBIT offers specific activities for setting up a training regarding business continuity. This requires a list of all personnel requiring training from the HR department of an organization. This is as follows:

- Training requirements have to be defined and maintained and plans for performing the planning of business continuity, impact and risk assessments, media communication and incident response. The training plans have to consider the frequency of training as well as the used training mechanisms.
- Competencies have to be developed based on practical training, which includes participation in tests and exercises.
- Skills and competencies based on the exercises and results have to be monitored.
- Users have to be trained periodically on malware in email and internet usage, to prevent users from installing shared or unapproved software.
- Awareness and training regarding the roles and responsibilities has to be provided on a regular basis. This is important so everyone in the organization knows the importance of their responsibilities, the role of controls, and the integrity, confidentiality, and privacy of the information of the organization (ISACA, 2012a).

Gap 2: Standardized reporting

Reporting incidents has to be done in a timely manner. The Wbni already presented a standardized form to report incidents. A similar version can be used to report incidents for NIS2. Kamara & Van Den Boom (2022) have created an example standardized reporting template. Healthcare organizations can use this to prepare for NIS2. This is presented in appendix 14.

There are three types of reports which have to be made (and reported in time): one within 24 hours of an occurred incident, one within 72 hours of an occurred incident, and one within 1 month of an occurred incident. Each report contains more details on the occurred incident (European Parliament, 2022). The details to be reported for each report (24 hours, 72 hours, 1 month) as well as the process flow are presented in appendix 16.

There will be a register where incidents have to be reported to. This register is currently not created yet (Overheid.nl, 2024). Therefore, keeping close contact with the CSIRT will ensure that correct registration for the register in a timely manner will be done.

Organizations can already prepare, however. This concept version states that organizations should provide the following information:

- The name of the organization;
- The address and actual contact information of the organization, which includes e-mail addresses, IP-reaches and phone numbers;
- If necessary, the sectors and subsectors of the organization which the organization belongs to, based on annex 1 or annex 2 of NIS2;
- If necessary, a mention of the states of the European Union where the organization provides its services towards based on annex 1 or annex 2 of NIS2;
- If necessary, the other mentioned by or pursuant to order in council information.
- The register will be published and opened the latest on the 17th of January, 2025 (Overheid.nl, 2024).

Gap 3: Contact with the CSIRT

Healthcare Organizations will have to set up contact with the CSIRT assigned to the healthcare sector. Z-CERT is the instance which is assigned to the healthcare sector. By creating the first contact as soon as possible, further improvements can potentially be made based on recommendations by the CSIRT. This is also important for future events which have to be attended to keep being up to date with the latest cybersecurity information and trends.

Gap 4: Standardized impact assessment

Since incidents will always have to be reported in a similar way, a standardized impact assessment report can be created. This has to be based upon the points presented in paragraph 2.2.3. Not only an assessment of the scale of incidents has to be made, but the incident also has to be reported in various ways.

For determining the actual severity of processes, the frameworks studied in the scope of this research are used. ITIL presents 11 activities regarding incident management[15]. This is presented in appendix 18. In appendix 19, a good practice or control/mitigation measure for each activity a control from one of the frameworks (or a combination of) is presented.

Gap 5: Mandatory cybersecurity risk education for management

[15] Incident management's purpose is to minimize the negative impact of incidents, by restoring normal service operation as quickly as possible (Leino, 2024).

Not only employees, but also management will have to participate in cybersecurity risk education. NIS2 requires this, so that all types of members (from the junior level functions all the way to the CEO/president) are able to identify and assess potential threats/risks. The Cbw (consultation version of the 21st of May) states the following:

- Each board member of an essential or important organization owns the knowledge and skills to:
- Be able to identify the risks regarding the security of network- and information systems;
- Be able to judge the risk control measures in the cybersecurity domain;
- Be able to judge the implications of the risks and risk control measures for services which is offered by the organization (Overheid.nl, 2024).

When a new board member enters the board, this person needs to be able to have all the above mentioned knowledge and skills within two years. Each board member also has to be able to prove this. An important aspect of this is that each board member needs to have a certificate of participation regarding training which deals with the above mentioned knowledge and skills (Overheid.nl, 2024).

Gap 6: Supply chain cybersecurity assessment

Since the entire supply chain of both information receiving and information sending parties which fall under NIS2 have to secure their supply chain, it is necessary to require stronger requirements from partner organizations. Since each type of organization is different, and since they may not even be in the scope of NIS2 at times, difficulties may arise. Therefore, an assessment on each individual partner organization regarding information security has to be done. This assessment has to look into how important the partner organization is for the daily operations of the healthcare organization, as well as what the impact is for the healthcare organization is when this information undergoes a cybersecurity incident.

BDO (2024) has created an analysis for dealing with this. Based on two axes, the impact times the risk of the delivery of information is looked at. An organization can be low impact, low delivery risk (routine), high impact, low delivery risk (lever), low impact, high delivery risk (bottleneck) or high impact, high delivery risk (strategic). To correctly categorize a partner organization, each of the NIS2 elements has to be looked at. A subset of measures/controls for NIS2 for each partner organization has to be looked at. By determining how ‘good’ or sufficient this is based on the standards required for the healthcare sector, a maturity assessment (for example, based on COBIT’s maturity model levels) can be done. When this determination process is done, new requirements to continue working together can be required from the partner organization. In other cases, the healthcare organization can choose to accept a risk (if an organization is not in the

scope of NIS2, for example) (BDO, 2024). This is also called a Kraljic matric, which is often used by procurement to deal with identifying and minimizing supply chain risks (Chartered Institute of Procurement & Supply, n.d.).

Appendix 15 presents BDO's Kraljic matrix, as well as an example of subset measures/controls for which has to be determined what maturity level they are. Healthcare organizations can use this approach to sufficiently prepare for the supply chain requirements required from NIS2. Requiring a certain level of cybersecurity controls from supply chain partners can be based on levels which are assigned to the matrix outcomes. An example of this would be the NIS2 quality mark, which offers four levels of cybersecurity to be implemented, which are basic, substantial, high, and finally ISO/NEN certification level (De Snoo, 2024). Organizations could require one of the levels from certain organizations in their supply chain to be in compliance with the Cbw based on their own risk assessment.

Regarding the supply chain cybersecurity, NIST states that the security control implementation includes assigning security capabilities provided by the selected security controls by an organization. Next to this, an organization should create clear communication lines among all affected parties, which are either providing or receiving the benefits of the implemented cybersecurity components. Because of this, the communication has to include the making certain that there is common control effectiveness, as well as audit results which are readily available and continuous monitoring. The supply chains which are directly affected by the common controls as well as with change management have to be informed in a timely manner. Therefore, organizations have to do the following:

- Provide a clear definition of all types of provided external services;
- Obtain detailed descriptions of how external services are protected, as well as conforming to the security requirements of an organization;
- Achieve sufficient assurance that the risk to the organization's operations, assets, and individuals stemming from the use of supply chain information (external services) is at an acceptable level (Kohnke et al., 2017).

COSO states that within process risks, the supply chain is one specific type of risk (Moeller, 2011). But other than this, not a lot surrounding supply chain risks is mentioned in COSO.

COBIT states a few management practices combined with some activities to make sure supply chain management is done correctly. As presented in appendix 13, the APO (Align, Plan and Organize) section can be used for this. COBIT starts off with mentioning that criteria regarding the type, criticality and significance of current suppliers and the corresponding contracts should be established and maintained over time. A focus on critical and important suppliers should be made. These suppliers should be evaluated and

compared for their performance over time. Next to this, COBIT mentions that risks relating to the supplier's ability to deliver their service in a secure, reliable, effective, continuous and in an efficient manner should be identified and monitored. When contracts are defined, potential service risks should be clearly defined based on service requirements. This includes alternative suppliers or temporary agreements to eliminate the possibility of supplier failure occurring, as well as to ensure security and protection of intellectual property (IP) and any legal or regulatory requirements. Finally, requesting independent reviews of the internal controls of the supplier is also important. For maintaining continuous improvement, a platform should be established to regularly communicate the need for and the benefits of continuous improvement.

To ensure that key suppliers and partners outside of the organization have effective continuity plans set up, audited evidence is required. Since this may be difficult, especially for smaller organizations, a NIS2 quality mark could be used. An example of this would be the NIS2 quality mark. This mark is based on three levels, basic, substantial and high (Stichting Kwaliteitsinnovatie, 2024). Organizations could require this specific quality mark to all, or a few, organizations in their supply chain. The problem is that the quality mark will only be available once the Dutch translation of NIS2 (the Cbw) is finalized and published (Samen Digitaal Veilig, 2024).

The good practice by DNB offers some good practices on third party and supplier management. Since these are very detailed, they have not been placed in this appendix.

Appendix 28: Turku University Data Management Plan

The research data management plan is based on the University of Glasgow's five questions. The questions are answered as follows:

1. What data will be created?
    a. Quantitative and qualitative data. Spoken data from the interviews and numbers from the survey.
2. How will the data be documented and described?
    a. The data will be documented in Word-files for each interview individually. The medium MS Teams will be used for this. The data will be analysed after all, or enough, interviews have been done and/or survey re-sponses have been collected.
3. How you will manage ethics and intellectual property rights?
    a. Every participant will be informed of the creation of the thesis, which will be published publicly. All data will be anonymised. The framework will be owned by both BDO and Alwin van Welie.
4. What are the plans for data sharing and access?

    a. Data won’t be shared, unless specifically needed in the thesis. No access will be granted to anyone whatsoever.

5. What is the strategy for long-term preservation and sustainability?
    a. After the thesis is completed, all material which may be traced back to the indi-vidual level will be deleted. Only anonymised and used data within the thesis will be kept.