Universiteit Leiden

ICT in Business and the Public Sector

Cybersecurity in the pension fund sector

Name: Dennis Prevaes
Student-no: S2350262

Date: 27/01/2021

1st supervisor: Joost Visser
2nd supervisor: Tino de Rijk

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Abstract

The pension sector is one of the vital financial infrastructures of the Netherlands. All pension funds combined manage a total invested capital of € 1,560 billion and process personal data of the majority of the Dutch population. This combination makes pension funds an attractive target for cybercriminals. However, information security and cybersecurity do not always seem to be a top priority for boards of pension funds. To effectively protect their assets, pension funds must become more cybercrime resilient.

This research examines the current state of information and cybersecurity within the pension sector in order to help pension funds become more cybercrime resilient.

A combination of theoretical background research, document review, surveys and gap analyses is applied to determine the required state and current state of pension funds regarding information and cybersecurity.

The required state of information security and cybersecurity of pension funds is determined through the use of document review.
As part of determining the required state, the DNB Good Practice framework is compared to the NIST framework. This comparison shows that the DNB Good Practice framework provides a good basis for managing information and cybersecurity, but falls short on the aspects of vulnerability management, incident management and awareness and control. In addition, the NIST framework is more descriptive and provides better handles for managing information and cybersecurity.

The current state of the identified topics is examined by surveying pension funds. Analysis of the survey results shows that the adoption rate of the DNB Good Practice framework is low and seems more driven by the supervisory authority than the intrinsic motivation of pension fund board members. Furthermore, pension funds appear to have insufficient knowledge and experience regarding IT safeguarded within their funds, making it more challenging to control information and cybersecurity related to their outsourced IT processes effectively. Finally, the governance domains of the pension funds are implemented by the responding pension funds but are not fully aligned.

Based on the identified gaps, improvements are devised. These improvements are incorporated within the ICS improvement model to help pension funds bridge these gaps. The ICS improvement model is designed based on the improvements and the best practices of the DNB Good Practice framework and the NIST framework.

This research shows that pension funds are not at the required level of cybercrime resilience. However, by combining the correct implementation of the DNB Good Practice framework with the designed ICS improvement model, pension funds can increase their cyber resilience.

Acknowledgements

Throughout the writing of this thesis, I have received a great deal of support and feedback. I am very grateful for the support of everyone who helped me. I would like to mention a few people explicitly.

Firstly, I would like to thank my first supervisor Joost Visser for continuous guidance during my thesis. Similarly, I would like to thank my supervisors from KoutersVanderMeer, Dennis Stabel and Joep Christiaanse for their insightful comments, feedback and the exciting discussions regarding the subject. Additionally, I would like to thank my second supervisor, Tino De Rijk and my colleague from KoutersVanderMeer Marcel Baveco, for their feedback regarding this thesis.

In addition, I would like to thank my friends and family for their support. You helped me to stay positive and focussed during some stressful moments writing my thesis. I would like to thank the “Dreamteam” (Rutger, Theo, Max and Ahmed) for their help and laughs, and my girlfriend Barbara for her continuous encouragement and support during my thesis.

I am very grateful for the people mentioned above, and also for those not explicitly mentioned that helped me during my thesis.

Dennis Prevaes

Table of content

Chapter 1: Introduction

1.1 Information and cybersecurity in the boardroom of pension funds

Nearly all vital processes and systems in the Netherlands are partly or entirely digitalised. With this, the dependence on IT increases. Specific processes are so essential to society that cyberattacks can directly damage the economy and society (National Cyber Security Centre, 2018).

The financial sector is part of the vital processes of the Netherlands. The following financial processes are marked as vital: counter payment traffic, massive cashless payment traffic, payments between banks and securities. Due to the high and large amounts of transactions that occur, a total or partial failure of these processes can have substantial social and financial-economic consequences (De Nederlandsche Bank, 2017). Because of the importance of the financial sector, The National Security Profile of the Netherlands has marked the financial sector as an attractive target for cybercriminals (Analistennetwerk Nationale Veiligheid, 2016).

The financial sector consists of three sectors: banking, insurance and pension. This research will focus on the pension sector. Since the pension sector is part of the financial sector, they are a vital process for the Netherlands (DNB, 2021). All pension funds combined have € 1560 billion in invested capital in early 2020 (DNB, 2020). Also, the funds process a significant amount of confidential personal data. This combination makes the pension sector an attractive target for cybercriminals. The pension sector is heavily reliant on trust; a cyber-attack where personal data is stolen, or timely payments are disturbed can cause significant damage.

In recent years there have been cyber-attacks that have affected the pension sector in the Netherlands. In 2017, WannaCry and NotPeyta malware occurred; this malware targeted various pension funds in the Netherlands. When the supervisory authority (DNB) investigated this, they stated that this malware was often handled effectively by pension funds. However, prior to these events pension funds had been victims of other forms of malware. The supervising authority concluded that information security was not yet at the required maturity level and that information security throughout the outsourcing chain is insufficient (DNB, 2018).

Outsourcing plays a critical role in the pension sector. Almost all pension funds have outsourced one or more activities to pension service providers. The outsourcing activities are diverse, such as pension management, asset management, management support and ICT (Talsma, 2018). This large-scale outsourcing has enabled pension funds to access more efficient and advances services and economies of scale. However, the other side of leaving work to external parties is that the knowledge and direct control of pension fund boards can decrease. This may cause an increased level of dependency for funds on their service providers. These dependencies are especially prevalent in the field of IT, where technological developments are mainly executed by the outsourced pension service provider. This could increase the distance and the level of dependency between the pension fund board and the pension service providers (Stabel D. , 2020).

Simultaneously the board of the pension fund has limited attention for and knowledge of IT risks. The combination of an increasing complex IT landscape, limited attention for IT risks, significant financial assets and sensitive personal data increases the risk of a potential cyberattack. DNB stated that the boards of pension funds are not paying enough attention to cybersecurity measures and do not have a clear overview of the potential (cyber)risks and the parties involved in the outsourcing chain (De Nederlandsche Bank, 2018). The subject of cybersecurity is not explicitly discussed in the board room, while the risk of a cyberattack is increasing.

1.2 Research questions

How can pension funds integrate cybersecurity and resilience in their critical business processes to ensure reliable and controlled business operations?

1. What are the cybersecurity requirements for pension funds and their managed service providers?
    a. What is expected from pension funds by the supervisory institutions and laws and regulations?
    b. What frameworks are available for managing cybersecurity?
2. How are the critical business processes of pension funds managed regarding information and cybersecurity?
    a. How do pension funds manage cybersecurity?
    b. What is the level of awareness and knowledge of board members of pension funds?
3. Is there a gap between the required state and the current state? If so, what are the steps that need to be taken to reach an adequate and proportional level of cyber resilience?
4. What instruments can be used to help pension funds reach an adequate and proportional level of cyber resilience?

1.3 Research approach

In this section, the general research strategy will be outlined. The research is divided into six phases. The complete research process, including the different phases, is illustrated below. In the following section, each phase is elaborated upon.

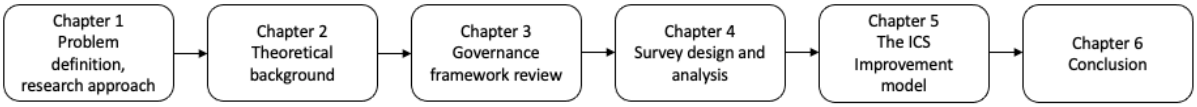

Figure 1: Schematic overview of the methodology

1.3.1 Problem definition and research approach

The first step in the research is the problem definition and research approach. The problem definition and research design are drafted in collaboration with KoutersVanderMeer. KoutersVanderMeer is a company that has an advising role in the financial sector in the Netherlands, especially in the pension sector. Explorative interviews are held with pension fund board members and experts on this topic to gain the proper context of the problem. The results of the explorative interviews can be found in appendix A. The language of the explorative interview was in Dutch, since the pension fund board members were Dutch and to avoid a language barrier.

1.3.2 Theoretical background

By having a preliminary research context, various concepts related to the research subject are identified. These concepts are examined during the theoretical background phase. The funnel method will be used to give more structure to the background research. This method starts with broad observations obtained from the explorative interviews, analyses the topics of the observations and then do an in-depth-research regarding the topics (Berthon, 2003). This method is used for the identification of the problems during the broad phase and to find the solutions in the analysis phase.

The theoretical background is written based on a combination of white and grey literature. White literature includes published journals, papers, conference proceedings and academic books. Grey literature includes governmental reports, lectures, white papers and news articles. White literature is used as much as possible in the theoretical background, but grey literature is used when scientific literature falls short.

This research used the ResearchGate database, University Leiden Database and Google Scholar as primary scientific literature sources. The research also uses "grey" literature like government documents, reports and research. The (combination of) keywords used to search the databases were amongst others: Pension fund, Cybersecurity, Board Room, Outsourcing, Information Security.

1.3.3 Governance framework review

The governance framework review phase will mainly focus on analysing policy documents, laws and regulations and cybersecurity frameworks to determine the required state for pension funds regarding information and cybersecurity. The following three topics were examined during the document review:

1. The DNB Good Practice framework
2. Knowledge, experience and countervailing power
3. The guidance documents of DNB (covering the governance domains)

The results of the document review phase provide the input for the survey.

1.3.4 Survey design and analysis

Survey

Based on the results of the document review, a survey is devised. The survey is distributed among 25 different pension funds, which covers around 10% of the pension sector. The survey is used as a quantitative method to gain insight into the pension funds' current state regarding information and cybersecurity. The candidates are individually approached using the network of KoutersVanderMeer. The language of the survey was Dutch, since all pension fund board members are Dutch and to avoid a language barrier.

The survey questions have undergone multiple iterations where the quality of the questions was checked. The pension fund experts at KoutersVanderMeer assisted in working through the various iterations of the survey questions. The survey design and questions can be found in appendix C

Gap analysis

A gap analysis is used in this research as a method of data analysis. The results of the document review and the results of the survey form the input for the gap analysis. The gap analysis method was chosen to compare the current state of pension funds regarding information and cybersecurity with the required state described in laws and regulations. Based on this comparison, possible gaps can be identified. By devising improvements and instruments to bridge these gaps, this research aims to improve the current state of information and cybersecurity for pension funds.

The gap analysis used in this research has five different steps and is linked to this research's sub-questions. The figure below shows a schematical overview of the gap analysis. Each of the steps will be further elaborated.

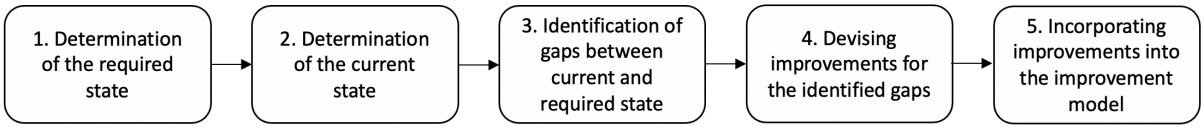

Figure 2. The schematic overview of the gap analysis used in this research.

Steps 1, 2, 3 and 4 of the gap analyses is performed in parallel. This means that the gap analysis is performed three times, once per main identified topic. The three topics are:

1. The DNB Good Practice framework
2. Knowledge, experience and countervailing power
3. Governance domains

The current state, identified gaps and improvements will be chronologically numbered, making it possible to refer back. The improvements devised in step 4 of the gap analysis is used as input for the improvement model.

The results of the gap analysis are validated with pension fund board members and with DNB. The validation is performed by short interviews regarding the results of the survey. This provided insight into the rationale to the answers of the survey. The language of the validation was in Dutch, since the pension fund board members are Dutch and to avoid a language barrier. In addition, DNB is approached for the validation of the survey results from the supervisory authority perspective. The results of the validation can be found in appendix C.

1.3.5 The ICS improvement model

Based on the devised improvements, the ICS improvement model will be developed.
This model gives a practical interpretation of the developed improvements and incorporates them into a plan-do-check-act model to ensure continuous improvement. The prototype of the model will be validated with the same method as described in the section above.

1.3.6 Conclusion

In the chapter conclusion, the research questions will be answered. In addition, the contributions, limitations and discussion of this research are presented.

1.4 Outline of this thesis

The outline of the theses is as follows:

- Chapter 1 describes the introduction; the research questions and the approach of this research.
- Chapter 2 describes the theoretical background of the research. The theoretical background focuses on the topics of information and cybersecurity, pension funds, the supervisory authority DNB and the DNB Good Practice framework. The theoretical background is primarily based on scientific and grey literature.
- Chapter 3 describes the different governance frameworks of pension funds. This includes the laws and regulations, the suitability requirements of pension fund board members, the IT governance domains of pension funds and the DNB Good Practice framework is compared to the NIST framework to examine information and cybersecurity requirements for pension funds.
- Chapter 4 describes the setup of the survey and the analysis based on the results of the survey. The survey is used to determine the current state of pension funds. The current state is compared with the required state, as described in chapter 3. Based on this analysis, gaps are identified and for the gaps are improvements devised. This analysis's three topics are the DNB Good Practice framework, suitability requirements for pension fund board members and the IT governance domains.
- Chapter 5 describes the ICS improvement model. This model is a practical interpretation of the improvements devised in chapter 4 and is incorporated into a plan-do-check-act cycle for continuous improvement.
- Chapter 6 describes the conclusion of this paper. This includes answers to the research questions, the contribution, limitations and future research.

Chapter 2: Theoretical background

Based on available white and grey literature, various concepts related to the thesis are analysed and discussed to provide insight into existing knowledge and theories. As a result, the theoretical background outlines a structured background for this thesis and gives it a scientific base. This chapter contains the following sections:

- Section 2.1 will discuss the concepts of information security, cybersecurity and cyber resilience.
- Section 2.2 will discuss various cyber frameworks
- Section 2.3 will discuss the various cyber threats the pension sector is facing.
- Section 2.4 will discuss pension funds and its related IT domains
- Section 2.5 will discuss the supervisory authorities and its duties
- Section 2.6 will discuss the DNB Good Practice framework

2.1 Security in cyberspace

In recent years the term "cyber" has been used to describe almost anything that has to do with networks and computers, especially in the security field (Ottis, 2010). This paper uses three different concepts are used regarding security in cyberspace: information security, cybersecurity and cyber resilience. Figure 3 shows the relation between the three concepts (Information Security Forum, 2011). This figure shows the core of the concepts information security, cybersecurity and cyber resilience is based upon confidentiality, integrity and availability (CIA).

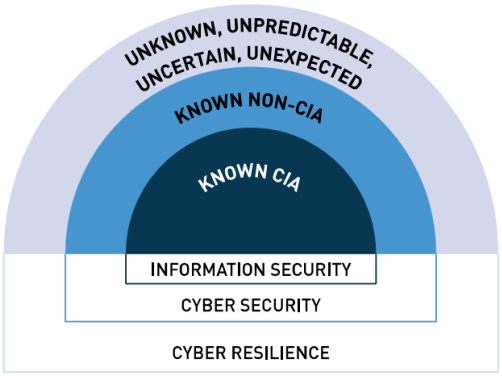

Figure 3 relationship between information security, cybersecurity and cyber resilience.

Securing cyberspace goes beyond these three core concepts. The "known CIA" is about the protection against threats that compromise the confidentiality, integrity and availability. The "Known Non-CIA" extends this boundary by including threats that are known but goes beyond the scope of confidentiality, integrity or availability. An example of this could be a cyber-attack on a powerplant, that not only compromises the CIA concepts but also affects society due to power outage. The last dimension, cyber resilience, is about threats that cannot be predicted, anticipated and mitigated and therefore focuses on the resilience despite (cyber)events. The three concepts are explored further in the following paragraphs.

Information Security

As displayed in figure 3, information security is based on the concepts of confidentiality, integrity and availability and has a narrower focus compared to cybersecurity. The concepts of information security can be found back in the following definition, where (Whitman, 2011) defines information security as “the protection of the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission”. This can be achieved via the application of policy, education, training and awareness and technology.

Cybersecurity

Cybersecurity goes beyond the boundaries of information security by not only including the protection of information resources but also that of other assets, including the person him/herself (Von Solms, 2013). It also includes the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and the assets of organisations and users (ITU, 2009). Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the nation's security, economy and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line, driving up costs and affecting revenue. It can harm an organisation's ability to innovate and to gain and maintain customers. Cybersecurity can be an essential and amplifying component of an organisation's overall risk management (NIST, 2018).

Cyber resilience

Cyber resilience can be defined as: "*the ability to continuously deliver the intended outcome despite adverse cyber events.*" (Björck, 2015). This ability can be considered from the perspective of different domains, ranging from a purely technical perspective to a national level, depending on the context. The notion of continuously means that the ability to deliver the intended outcome should be working even when the regular delivery mechanisms have failed. The intended outcome refers to the outcome that was intended to achieve. This can be a business goal, process or service delivered. Adverse cyber events refer to all events that negatively impact the availability, integrity or confidentiality of networked IT systems and associated information and services.

Comparison

The term cybersecurity is often used interchangeably with the term information security, although these two concepts are not totally analogous. In information security, the assets that need to be protected is the information and all its aspects. This includes the underlying ICT assets and goes beyond just technology to include information that is not stored or communicated directly. In cybersecurity, the assets that need to be protected can range from persons to household appliances to society at large. These assets include anyone or anything that can be reached from cyberspace. There is a substantial overlap between cybersecurity and information security including the CIA concepts however cybersecurity goes beyond the boundaries of traditional information security to include not only the protection of information resources but also that of other assets, including humans, electronic devices or society that can be reached through cyberspace (Von Solms, 2013).

As described above, cybersecurity is generally focussed on the protection of its assets; this differs from the focus of cyber resilience. The focus of cyber resilience is on a higher level by ensuring business delivery. Cyber resilience takes the business value as its starting point, while cybersecurity uses information technology. A company is cyber resilient if it is able to deliver business value, even when faced with adverse cyber events. The intention of cybersecurity is to design or protect systems so that they have the property of being fail-safe, while the intention of cyber resilience is that a system has the property of safe-to-fail. (Björck, 2015).

Figure 3 shows that all three concepts are related to each other. Each concept is an extension of to the previous one. Cybersecurity adds an additional dimension to information security by including human assets. Cyber resilience adds an additional dimension to cybersecurity by ensuring business delivery in addition to the protection of assets.

2.2 Information and cybersecurity frameworks

Various cybersecurity framework exists to help enterprises integrate structures and to manage cybersecurity effectively and methodically. This chapter will examine three different frameworks and compare them to each other in order to find the best practices and requirements to be able to manage cybersecurity effectively.

ISO 27001

The ISO 27000 family of standards offers a set of specification, codes of conduct and best-practice guidelines for the organisation to ensure strong information security management. ISO 27001 is based on the plan-do-check-act (PDCA cycle) for continuous improvement.
ISO 27001 offers a structured approach of developing an ISMS and the specification of features an effective information security system should possess (Disterer G. , 2013).

NIST framework

The NIST Cybersecurity Framework provides guidance on how an organisation can improve its ability to prevent, detect and respond to cyberattacks and threats. The NIST framework has a risk-based approach to managing cybersecurity. Through a process of continuous improvement, the NIST framework incorporates advanced cybersecurity technologies and practices within the organisation (NIST, 2018).

COBIT

COBIT (Control Objectives for Information and Related Technology) is a high-level framework for the governance and management of enterprise information and technology aimed at the whole enterprise. COBIT contains 34 IT processes, each with high-level control objectives and a set of detailed control objectives. These controls are grouped in 4 domains: plan and organise, acquire and implement, deliver and support and monitor (Arora, 2010). COBIT addresses the modern technologies, trends and security requirements for organisations. It brings together six principles that allows enterprises to build an effective governance and management framework positioned in a holistic set of seven enablers that optimise information and technology investment and use for the benefit of stakeholders(ISACA, 2019).

Comparison between frameworks

The intention of the three different frameworks is the same, to help defend the organisation against cyber events. The overlap between the frameworks is that they all focus on continuous improvement and use of a variation of the plan-do-check-act cycle. However, there are several differences between the frameworks.

COBIT is a high-level principle-based framework that emphasizes on the management and governance of IT. Information and cybersecurity are incorporated into the framework but is not the core focus of the framework.

ISO 27001 focusses on the creation of an information Security Management System that helps companies to continuously improve their information security. ISO 27001 places more emphases on the information security aspects than the cybersecurity aspects. In comparison to NIST and COBIT, ISO 27001 is the only one that is certifiable (Arora, 2010).The NIST framework focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of the organisation's risk management process. The NIST framework uses best practices from other frameworks like COBIT and ISO 27001.

To conclude, COBIT is a more high-level framework for managing IT, ISO 27001 is more detailed on implementing an information security management system and NIST is in the middle of these frameworks, by combining best practices from both frameworks to manage cybersecurity (NIST, 2018).

2.3 Information and cyber threats in the pension sector

As mentioned, the pension of the Netherlands sector has a combined €1560 billions of invested capital. In addition, the funds process a significant amount of confidential personal data. This data includes names, addresses, bank details and health data. The combination of these two factors makes the pension sector an attractive target for cybercriminals. The pension sector in the Netherlands has not yet fallen victim to major cyber-attacks, but institutions with similar characteristics have been. For example, the University of Maastricht who holds personal data of 24.500 students and employees, have fallen prone to a ransomware attack forcing the University to pay 200.000 euro to the hackers (NOS, 2020). More recently, the National Health Service of the UK (NHS), who possess personal information of UK citizens, was targeted with over 40000 phishing emails during the corona crisis (Healthcare Dive, 2020). In addition, the NHS was also targeted with the WannaCry malware in 2017 resulting in a financial loss of 35 million pounds (S. Ghafur, 2019). The examples above show that institutions with similar characteristics have been successfully attacked by cybercriminals.
The impact caused by cybercriminals depends on the type and scale of the attacks; it could include any of the following:

- Interruption of the pension service where payments are delayed, which has a direct impact on the pensioners.
- Reputational damage which could lead to loss of affiliated employers and confidence in the fund.
- Loss or disclosure of member data which could lead to regulatory actions and significant fines.
- Time to restore systems and software affected by the attack
- Financial costs, including direct theft of money and the costs of restoring and repairing

In the following section the five most dominant cyber threats for pension funds (DNB, 2018) and the potential damage it could cause are discussed. These are just five of the common cyber threats identified by DNB, there are many more threats.

Distributed denial of service

In a distributed denial-of-service (DoS) attack, the attacker sends a large number of connection or information request to a target. These requests are sent in such a high volume that the target system becomes overloaded and cannot respond to a legitimate request for service or becomes unable to perform its normal functions (Whitman, 2011). A DDoS attack could potentially disrupt pension payment services for an extended period of time affection the pensioners reliable on the pension pay-outs. If the DDoS attack persists for an extended period of time, the fund could face reputational damage, as well as the loss of confidence by pensioners. If the DDoS attack happened due to lack of cybersecurity and personal information is stolen, the pension fund could also be fined by the privacy supervisor.

Unauthorised access

Unauthorised access is trying to gain privileged access using someone else's account or other methods. Financial institutions increasingly outsource parts of their vital infrastructure and services to third parties. Organised crime groups can gain access to the core system of the financial institution through outsourced services (1FTL-NL, 2019). Especially pension funds with a high percentage of outsourcing, including third parties, are vulnerable to this type of cyber threat. The personal data and financial assets are managed by service providers who frequently outsource data storage to third parties. If these third parties are insufficiently protected, cyber criminals can break into the system and can access the data of pension funds.

Accidental data leakage / corruption

Data leakage is the unauthorised transmission of data from within the organisation to an external party. The data can be transferred electronically or physically; usually, data leaks occur via the web and email but can also occur via mobile devices and data storage devices. It can also occur that employees are selling or deleting data for their own personal gain. An example of (accidental) leakage for the pension could be that people can see other people's pension statements due to a bug in the system.

Phishing

Phishing is a form of identity theft that is a combination of social engineering and sophisticated attack vectors to obtain personal credentials or financial information of victims. The victim is tempted by the phisher to click on a rogue URL and leave their personal details (Cui, 2017). The phishing method can be effective because it is aimed at provoking human behaviour. A computer can be protected by technical means, but an individual can't. Phishing is often the first step in a chain of steps to carry out a targeted attack on an individual or organisation. Phishing is dangerous for pension funds ranging from the internal employees as for the participants of the fund. Employees can be tricked into providing login details, where cybercriminals could access personal data of the participants. Participants of the fund can be tricked into providing login and account detail to cybercriminals who can alter their pension plans for personal gain. Both sides are vulnerable to click a rogue link or by entering their credentials at a false website.

Brute force attack

A brute force attack is a method of using computational power to try every possible password combination to gain access. Brute force can be used to gain access to parts of the IT infrastructure of pension funds or accounts of participants.

2.4 Pension funds

By having a clear understanding of all the cyber components and the threats pension funds are facing, the pension sector of the Netherlands will be further elaborated upon. In the figure below a simplified structure of pension funds is displayed. In this structure, the pension fund board is the ultimate responsible party supervised by DNB. In general pension funds have management support and outsource the pension fund administration and the asset management to pension service providers. In the following sections, the pension fund and its components will be examined in order to combine the topics of cybersecurity and pension funds in the last section.

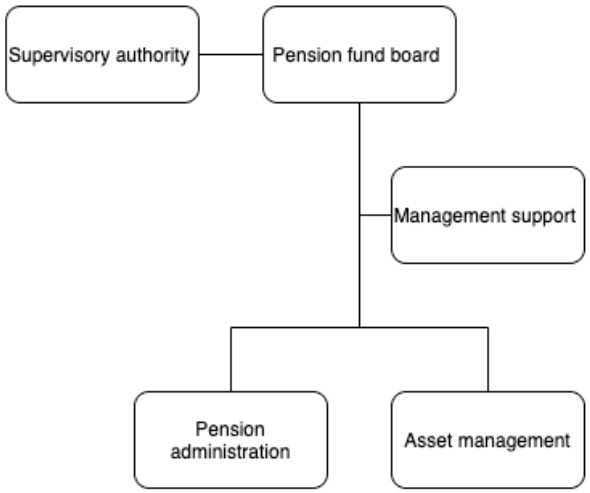

Figure 4: Simplified structure of a pension fund, including the three main IT-domains and the supervisory authority.

Pension fund

A pension fund is an organisation that collects pension contributions of members of the fund, subsequently invests the collected money, and later on performs the pay-out of pensions to people who retire. In the Netherlands, most pension funds are linked to one employer, but there are also pension funds that administer the pensions of an entire industry. A pension fund is a financial institution and therefore must comply with Dutch and European laws and regulations and is supervised by DNB.

Governance of pension funds

Board members of pension funds are appointed by or on behalf of employers, employees and retirees. One of the aims in regard to the composition of a pension fund board is to consist of a diverse group of people with different areas of expertise. The majority of the pension funds in the Netherlands have board suitability policies in place, stating that members of the board need to have expertise in areas such as managing organisations, laws and regulations, pension plans and types, financial aspects of pension plans, asset management and risk management, administrative organisation and internal control, communication and outsourcing (Pensioen Federatie, 2014). This does not include knowledge and experience requirements regarding ICT. The head of the department of supervision of pension funds states that IT expertise and attention under board members is limited (DNB, 2020).

Critical business processes

Pension funds have two critical business processes. The critical business processes are the administration of pension and the management of the assets of the fund's participants. These critical business processes are, in general, outsourced to managed service providers. The pension fund has the legally required task to manage this outsourcing since they are ultimately responsible. In order to manage the outsourced activities pension funds must have enough countervailing power safeguarded within the board to be in control of the outsourcing relationship. This includes that the pension fund must have expertise and knowledge safeguarded for managing the outsourced relationship. They use the expertise and knowledge in combination with accountability reports for the monitoring, evaluation and the adjustment of the outsourced activities. These accountability reports provide information on how the managed service provider managed the outsourced processes of the fund. Based on the evidence from the accountability reports, the pension fund demonstrates to the supervisory authority that they have safeguarded their critical business processes within the fund.

Outsourcing

Pension funds strive to achieve the best results possible at relatively low costs. This is for the benefit of the participants, retirees and employers. Outsourcing helps to achieve this. In recent years, pension funds have been able to gain access to more efficient and advanced services and economies of scale through large-scale outsourcing. Pension funds outsource many of their critical business processes to managed service providers. One of the downsides of outsourcing is that the knowledge and direct control of pension fund boards may decrease. In addition, dependencies can arise between the pension fund and their managed service providers (Staatssecretaris van sociale zaken en werkgelegenheid, 2014). There has been an increase in outsourcing over recent years (DNB, 2018). The IT landscape is changing and is becoming more complex; parts of the IT used by pension funds is outsourced to, for example, cloud providers (Stabel D. B., 2020) (DNB, 2018). The outsourcing of pension service providers contributes to a longer and more complex outsourcing chain.

In scientific literature, the following is stated regarding outsourcing: “The complexity and connectivity of information systems and networks has been increasing over the years” (Merali, 2006). It is common that organisations are no longer able to perform all their tasks independently. Therefore, organisations outsource their tasks and become dependent on other organisations for the delivery of data, support or data processing. One of the primary reasons why outsourcing has become popular is cost reduction (Belcourt, 2006). Nowadays, this is not the only motivation for organisations to outsource. Other reasons for outsourcing are increased focus on core business processes, access to talent and a skilled and highly available workforce and (Kakabadse, 2005). Despite the benefits associated with outsourcing, there are also risks being considered. Examples of outsourcing risks are the possibility of weak management, miscommunication, hidden costs and business uncertainty (Earl, 1996).

The findings in the scientific literature regarding the benefits and risks associated with outsourcing can be substantiated with grey literature. A benefit of outsourcing is that pension funds can get access to more efficient and advances services, expertise and economies of scale (Talsma, 2018). The downside of outsourcing processes to service providers is that the knowledge, expertise and direct control pension fund boards have can decrease. In addition, dependency relationships can arise between the pension fund and their service provider (Klijnsma, 2014). Pension service providers are also increasingly using outsourcing for their activities, especially in regard to IT.

Pension fund IT domains

Pension funds who use outsourcing, outsource their critical business processes to managed service providers. This includes the IT that supports these activities. Pension funds and their service providers deal with sensitive personal information and must therefore safeguard the confidentiality, integrity and availability of the data. In general pension funds have three different IT domains that support the critical business processes:

1. Boardroom
2. Asset management
3. Pension administration

IT domain: Boardroom

The administrative environment includes the board and the supporting staff of the pension fund. The main task of the board is to ensure that the pension fund is properly managed. This includes the management of the critical business processes. The board is responsible for managing the risks pension funds, including IT and outsourcing risks. The IT domain of the boardroom is set up to support the activities of board members of the pension fund, like meetings, dashboards or file sharing tools.

IT domain: Asset management

The asset management environment manages the money of the pension funds participants. The goal is to increase the invested money of the fund' participants to provide a good income for when the participants retire. The IT domain of the asset management contains all the components that make it possible to make the transactions for the investments. The management of assets is one of the critical business processes since it manages all the money of the pension fund's participants.

IT domain: Pension administration

The pension administration environment manages the administration, arranges the automation of collections and pay-out of premiums of the fund and the communication between participants and the pension fund. The IT domain of the pension administration supports all the critical business processes of the pension administration and the pension fund. The IT domain of the pension administration processes personal data of the pension fund's participants and must therefore be well protected. As one of the tasks of the pension administration, they provide the associated pension fund with accountability reports stating how their critical business processes are managed. The pension administration is not supervised by the DNB, but the DNB especially focusses on the outsourcing relationship of the pension fund with their pension administration due to the highly sensitive data it processes.

Pension fund ISAC

The pension fund ISAC is an Information Sharing and Analysis Centre (ISAC) that helps pension funds to share information relevant to the pension sector. An ISAC can play an important role for the provision of information regarding sectoral incidents, threats, vulnerabilities and controls regarding information and cybersecurity. A pension fund ISAC can collect and distribute relevant sectoral information regarding information and cybersecurity from the IT domains of pension funds. If affiliated, pension funds can use this information to improve their information and cybersecurity by asking critical questions to their managed service providers.

2.5 Supervisory authority

De Nederlandsche Bank (DNB) is the supervisory authority of various financial institutions of the Netherlands. DNB serves as the Dutch central bank and aims to ensure the financial stability of the Netherlands. In order to achieve this, DNB supervises banks, pension funds, insurers and other financial institutions in the Netherlands. One of the tasks of DNB related to pension funds is the assessment of board members and the ongoing supervision of pension funds.

Assessment of pension fund board members

One of the tasks of DNB is to assess the suitability and reliability of administrators and policymakers for financial institutions. The requirements policymakers must meet are stated in the policy on suitability 2012 (Overheid, 2020). When assessing suitability, DNB determines whether the candidate has sufficient relevant knowledge, skills and professional behaviour and various other competencies (e.g. independence, persuasion, cooperative power, decisiveness) to be able to fulfil the position. This is evident from, among other things, education, work experience and competences. Suitability is assessed on the basis of information supplied by financial institutions and an assessment by DNB.

Open book supervision

One of the other tasks of DNB is the ongoing supervision of pension funds. DNB uses Open Book Supervision and wants to increase the awareness of the applicable laws and regulations: partly by presenting the laws and regulations in an accessible and coherent manner and in part by brief explanations of those laws and regulations. Open Book Supervision is the web-based information desk on DNB's regulations, implementation and policy with regard to prudential supervision. For the open book supervision, DNB has drafted a guidance document that provides a practical interpretation for governance domains of pension funds that comply with laws and regulations.

For the compliance with the laws and regulation regarding information and cybersecurity, DNB made a framework, hereafter called the 'the DNB Good Practice framework', which will be elaborated upon in the following section.

For the implementation and supervision, DNB assesses the pension funds proportional to the size of the fund. The size of the fund is categorised based on the proportionality ladder of DNB. The ladder is based on the risk classification of the funds and distinguishes the following proportionality classes:

- T1 is in principle limited to (automated) analysis of statutory financial standards, such as the funding ratio of pension funds or the solvency ratio with insurers and are occasionally included in thematic research.
- T2 institutions also use reports and analyses as the main sources of information, but the T2 institutions do participate in DNB-wide theme projects.
- T3 institutions get standard assessments of the business model & strategy, culture, behaviour & governance, infrastructure & IT and general risk management. For the settings in T2 and T3, the risk analysis basically relates to a group of institutions with similar characteristics. A supervision plan is drawn up for each group and the relevant ones are drawn up risks selected. In T3, institution-specific risks can also be included in the supervision plan.
- T4 are the largest institutions and per institution, a supervision plan is drawn up due to the complexity and the associated risks. (DNB, 2012)

2.6 The DNB Good Practice framework

The DNB Good Practice framework provides pension funds under supervision with practical guidance on the implementation of control measures to ensure the integrity, continuous availability and security of electronic data processing. The DNB Good Practice framework is developed in 2010 and annually adjusted based on current developments. In 2019 DNB added specific cybersecurity components to the DNB Good Practice framework

The DNB Good Practice framework consists of 8 different elements, 58 controls, a risk management cycle and a maturity model. All the different aspects of The DNB Good Practice will be explained below. The DNB Good Practice framework has origins from different information and cybersecurity frameworks like COBIT, ISO and NIST.

Elements

The following eight elements form the basis of the self-assessment framework.

Table 1: Elements of the DNB Good Practice

Element	Description
1. Governance	Governance is about the preparation, maintenance and the dissemination of an information security policy where tasks and responsibilities are formally described.
2. Organisation	The element organisation pays attention to documenting and formalising roles and responsibilities for risk and information security management.
3. People	The human factor is very important for the control of information and cybersecurity. The element people focus on attracting and retaining employees with knowledge of information and cybersecurity.
4. Processes	The processing element focusses on the IT-continuity plan with the aim of reducing the impact if one of the key business functions is disrupted.
5. Technology	The Technology element focusses on ensuring that control measures are arranged to have a high level of availability, confidentiality and integrity. Hereby taken into account the cyber risks the institution faces.
6. Facilities	The facilities element is focussed that the institution has a policy that is defined, is implemented and is regular updated regarding physical security and obtaining access to office buildings and areas.
7. Outsourcing	The outsourcing element focusses on that the institution has made adequate outsourcing processes with service providers regarding information security, assurance and risks reports.
8. Testing	The testing element focusses on the type, scope and depth of tests the institution performs based on the risk profile of the institution.

Controls

The control measures are categorised per element. Per element, there is a short summary of the most important control measures with examples. The control measures focus on the perspective of the pension fund board and on the role of the board regarding the implementation and the supervision of those control measures.

Risk Management Cycle

The risk management cycle applies to all elements of the framework. Pension funds need to periodically evaluate to what extend the control measures taken are effective in dealing with the constant changing risks in the field of information and cybersecurity. Based on the risks assessment, the pension fund determines its response and takes measures to limit risks and accepts (temporary) residual risks. This risk management cycle is based on the plan-do-check-act cycle or the Deming cycle. This cycle described four activities that apply improvements within an organisation. The cyclical nature of the cycle guarantees that quality improvement is constantly under attention.

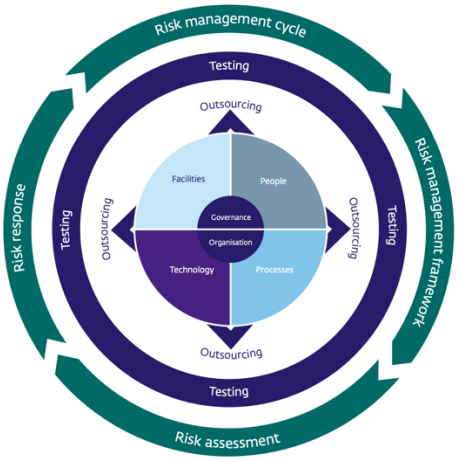

Figure 5: The risk management cycle of the DNB Good Practice framework

DNB Good Practice framework self-assessment

The DNB has for years been investigating the quality of information and cybersecurity as a theme within the financial sector. In order to investigate this theme, and as part of the supervision, the DNB has pension funds complete self-assessments. The purpose of the self-assessment is to determine to what extent the control of information security and cybersecurity is at the required level. To determine this level, DNB uses a maturity model.

Maturity Model

DNB requires that all pension funds are demonstrably in control. The DNB Good Practice framework and self-assessment contain 58 control measures. Pension funds must score at least maturity level 3 on 55 of the control measures and maturity level 4 on 3 control measures. The control measures: 4.1, 4.2 and 4.3 are from the category IT risk management. The aim of this is to ensure that the pension funds have their risk management and risk identification in order which in turn acts as the basis for the other control measures (Baveco, 2015). In order to comply with sound and ethical business operations, the pension funds must reach the required maturity level of all controls. The maturity levels are described below.

Table 2: Maturity model in the DNB Good Practice Framework

Level	Definition maturity level
0	Non-existent - No attention was paid to this control measure.
1	Initial - The control measure is (partially) defined but is performed inconsistently. There is a significant dependence on individuals in the implementation of the control measure.
2	Repeatable but informal - The control measure is in place and will be implemented in a consistent and structured but informal manner.
3	Defined - The design of the control measure is documented and is implemented in a structured and formalised manner. The required effectiveness of the control measure can be demonstrated and is being tested.
4	Controlled and measurable - The effectiveness of the control measure is periodically evaluated. Where necessary, the control measure is improved or replaced by another control measure. The evaluation of the control measures is recorded.
5	Continuous improvement - The control measures are anchored in the integrated risk management framework, with continuous efforts to improve the effectiveness of the measures. External data and benchmarking are used for this. Employees are proactively involved in improving control measures

Information security monitor

Every year the DNB published the information security monitor (IB monitor) were the most important observation regarding information and cybersecurity aspects that can be improved. The IB monitor emphasizes on these observations with the aim that pension funds tackle these aspects within their fund. The IB monitor is based on results from the theme-oriented supervision at pension funds. The current IB monitor has made the following observations regarding information and cybersecurity:

- Cyber hygiene and vulnerability management, in particular, remain crucial
- Testing measures contribute to the continuous improvement of cyber resilience.
- Stay in control over the fund's outsourced activities.
- Prevention alone is not enough; the focus is shifting towards detection and response.
- Be aware of the role you have as a board member regarding information and cyber security.
- Be aware of specific risks that emerge from the COVID-19 pandemic.

Chapter 3: Review of governance frameworks

This chapter examines the governance frameworks applicable to pension funds. A top-down approach is used for the examination where first, the legal frameworks are outlined. Secondly, the suitability requirements of pension fund board members are examined.
Thirdly, the governance domains: IRM, outsourcing and IT are examined. At last, the specific information and cybersecurity of pension funds requirements are examined. This examination is done by comparing the requirements of the DNB Good Practice framework with the NIST framework. The choice of the NIST framework is substantiated later in this chapter. By combining all the examined elements, the required state of information and cybersecurity can be determined. The required state will be used in chapter 4 in the gap analysis.

3.1 Laws and regulations

Laws and regulation indicate the legal requirements that pension fund must comply with.
The following laws and regulation have been identified as relevant for pension funds managing information and cybersecurity.

- Article 143 of the pension act
- Article 34 of the pension act
- Article 3.17 of the financial supervision act.
- Policy rule 2012 on suitability

Article 143 of the pension act.

Article 143 states that pension organise their pension fund in such a way that controlled and sound business operations are safeguarded. This law related to the following aspects of a pension fund:

- Rules are defined for controlling business processes and business risks.
- Controlling includes the entire process of planning, controlling, monitoring and adjusting objectives and processes.
- Pension funds must have a clear organisational structure and clear reporting lines, which is a precondition for controlled processes.

Article 34 of the pension act.

Article 34 of the pension act state the pension funds are permitted to use outsourcing if they comply with the following:

- Pension funds remain ultimately responsible for the outsourced activities
- Contractual agreements are drafted regarding the outsourced services
- Enough countervailing power (knowledge and experience) is safeguarded within the pension fund board to keep control over the outsourced activities and make timely adjustments. (DNB, 2020).

Article 3.17 of the financial supervision act.

Pursuant to the Financial Supervision Act (explained in more detail in the supervisory authority chapter) and the Pensions Act, DNB holds that financial institutions must have adequate procedures and measures in place to control IT risks. "Adequate" is taken to mean that the procedures must be in line with the nature of the financial institution and the complexity of its organisational structure. DNB emphasizes the importance of the alignment between business and IT.

Policy rule 2012 on suitability

The policy rule 2012 on suitability clarifies what the regulator (DNB) understands by "suitability" and which aspects are taken into account in the assessment of the pension fund board member. The policy rule also provides clarity regarding requirements which persons must meet in order to become a pension fund board member.

3.2 Knowledge, experience and countervailing power

One of the tasks of the supervisory authority, DNB is to assess the suitability and reliability of administrators and policymakers for financial institutions. The requirements policymakers must comply with are stated in the suitability plans. When assessing suitability, DNB determines whether the candidate has sufficient relevant knowledge, skills and professional behaviour and various other competencies (e.g., independence, persuasion, cooperative power, decisiveness) to be able to fulfil the position. This is evident from, among other things, education, work experience and competences. Suitability is assessed based on information supplied by the pension fund and by assessment of DNB.

Suitability requirements for pension fund board members

The assessment of the suitability of the candidate by DNB is based on five focus areas from the Policy Rule on Suitability 2012:

- Management, organisation and communication.
- Products, services and markets in which the organisation operates.
- Sound and ethical business operations.
- Balanced and consistent decision-making.
- Sufficient time.

For pension fund directors that hold key functions (risk management, internal audit and actuarial function) specific suitability requirements apply. The following requirements regarding expertise and knowledge of IT apply to the key function holders (De Nederlansche Bank, 23):

- Risk Management function:
    - Broad knowledge of the most important IT risks and relevant technological developments that affect pension funds.
    - No specification of relevant education and work experience which is IT-related.
- Internal Audit function:
    - Considering the breadth of the area of attention, the key function holder does not need to have in-depth expertise in all areas of knowledge. The key function holder must be able to assign more specialist tasks within his responsibilities to persons who perform work for the key function.
    - Persons who meet (amongst others) the professional rules of the NOREA (titles RE or CISA) and who may bear the corresponding title are deemed to have the required professional knowledge for the performance of the function of key function holder Internal Audit. However, such a title is not required.
- Actuarial function: no further explanation by DNB.

The DNB emphasizes that the requirements of knowledge, experience and countervailing power must be appropriate to the scope, nature, scale and complexity of the pension fund. The proportional application of the required degree of depth in the various knowledge areas is assessed per situation (De Nederlansche Bank, 23).

3.3 Governance domains of pension funds

DNB provides guidance documents that provide a practical interpretation of the laws and regulations in order to assist financial institutions be compliant. These guidance documents focus on the different governance domains of pension funds. DNB describes the following three guidance documents:

Guidance document	Governance domain	Description
The DNB Good Practice: Outsourcing	Outsourcing	The DNB Good Practice outsourcing helps pension funds to manage and maintain outsourcing relationships.
The DNB Good Practice: Integrated risk management IRM	Integrated risk management	The DNB Good Practice IRM helps pension funds to manage risks in an integrated manner.
The DNB Good Practice: Information security	Information security, IT policy	The DNB Good Practice information security helps pension funds managing their information and cybersecurity by providing controls and a self-assessment framework. The purpose of the self-assessment is to determine the maturity level of the pension fund.

Table 3: Guidance documents, domains and description

The relation between these topics can be illustrated with the IT governance alignment model, as seen in the illustration below.

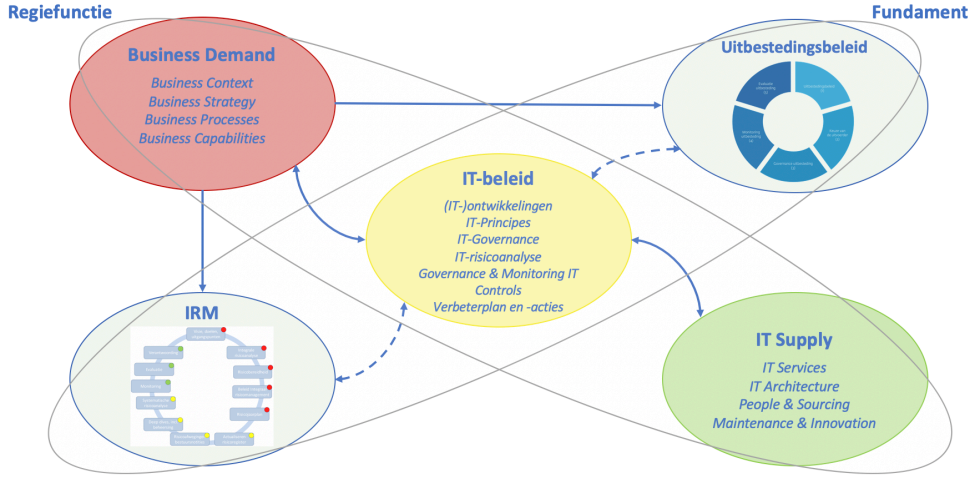

Figure 6: The alignment between the IT policy and the other pension fund governance domains by D. Stabel.

The model describes how pension funds can operationalize the management of their IT function. The model illustrated how the different governance domains IT policy, IRM and outsourcing contribute to the alignment between the business demand and the IT supply of pension funds. Pension funds are in control over their IT governance if they have the following:

- Integration of the IT policy into the governance domains of IRM and outsourcing
- IT policy integrated with the strategy of the pension fund
- The IT governance domains contribute to the outsourcing relationship between pension fund (business demands) and managed service providers (IT supply).

The alignment between the business demand and the IT supply is based on the COBIT principles 1 and 2:

1. Stakeholders. Where the IT function should contribute to the value creation of the organisations
2. Business and IT are interwoven. Where the IT function is integrated into the management of the entire business.

The different governance domains will be further explored in the following sections.

IT policy

IT is a precondition for the implementation of efficient and effective business processes. The development of IT contributes to the improvement of business operations and the strategy of the fund. At the same time, the deployment of IT involves specific risks. An IT policy can help pension funds to take advantage of the opportunities offered by IT and to manage the IT risks. The IT policy describes the way pension funds want to deal with its IT function and the management of related risks. A clear vision and strategy on IT, IT outsourcing and IT risk management contributes to the functioning of pension funds. The IT policy should be seen in conjunction with the two other governance domains: IRM and outsourcing.

Integrated Risk Management (IRM)

Integrated risk management is about the way organisations have set up their risk management. This includes strategy, policy, processes, procedures, embedding in business operations, division of capacity and responsibilities and independent assessment.
In combination with the operation of risk management they cover the management of all the different risk areas in a mutual connection. The integrated approach emphasizes that it concerns the management of all the different risk areas in mutual cohesion. Integrated risk management is a continuous iterative process of:

1. Updating the IRM policy
2. Identification of risks
3. Risk assessment
4. Implementation of risk measures
5. Monitoring of the risk measures
6. Evaluation of the risk measures

Figure 7: Visual representation of the IRM cycle.

The DNB guidance document describes how pension funds should implement the IRM process, as described above and emphasizes the following points:

- Board members are committed to IRM
- Sufficient countervailing power must be safeguarded within the board
- IRM must be proportionally aligned with the strategy and the risk appetite of the pension fund.
- The risk management processes must be periodically updated and evaluated.
- The pension fund must have a complete overview of all relevant risk and the underlying coherence with other risks.

To properly implement IRM as a pension funds the following aspects must be sufficiently incorporated within the fund:

- Risk appetite
- Overview of the IT landscape
- Risk assessment

Risk appetite

A risk appetite describes the level of risks the organization is willing to accept to achieve their strategic goals and objectives. The risk appetite must be aligned with the strategy of the fund and must have defined a risk appetite scale. The scale describes the risk approach of the fund ranging from risk seeking to risk averse (Dixon, 2017).

The IT risk appetite describes how the fund deals with IT related risks where the DNB has defined the following focus area's

- Confidentiality
- Integrity
- Availability

For each IT risk, the fund must determine how it could affect the confidentiality, integrity or the availability of the pension fund. For example, pension funds store a large amount of sensitive data of their participants. The top priority of the pension funds is to ensure that the confidentiality and integrity is guaranteed. In order to achieve this, the pension fund must have control in place that mitigate the risk of losing the confidentiality and integrity of the data.

Overview of the IT landscape

The complete IT landscape must be identified in order to effectively assess the IT risks. The IT landscape includes the used applications per outsourced service, critical outsourced services and location of stored data. The IT landscape must be identified for the managed service providers of the pension funds and the 3rd party service providers that the managed service providers are using.

IT Risk assessment

Once the risk appetite of the fund is defined and the complete IT landscape is identified the IT risk assessment can be performed. The IT risk assessment includes the identification of risks, the assessment of the risks and the monitoring and evaluation of the control that mitigate the risks. For each identified risk, controls are implemented to mitigate the risk based on the risk appetite of the pension fund. The effectiveness of the controls are assessed and based on the assessment the control can be adjusted. The assessment of the risks is done by monitoring and evaluating accountability reports obtained from managed service providers.

Outsourcing policy

DNB guidance document describes how pension fund should organize their outsourcing processes in order to comply with the laws and regulations regarding outsourcing.

The outsourcing processes is an iterative and continuous process to safeguard a sound and controlled outsourcing relationship between pension funds and the managed service providers. The outsourcing process contains the following steps:

1. Establish an outsourcing policy
2. Choosing the outsourcing party
3. Governance of outsourcing
4. Monitoring of outsourcing
5. Evaluation of outsourcing

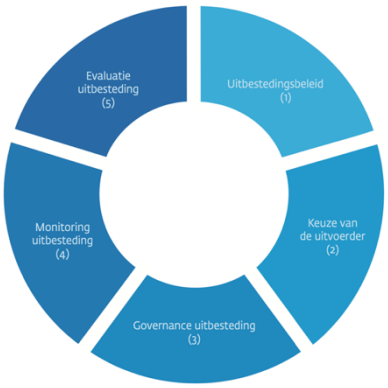

Figure 8: The outsourcing cycle

The DNB Guidance document: outsourcing emphasizes the following aspects:

- Pension funds must have an outsourcing policy in place that contains requirements where managed service providers must comply with. This includes financial stability, sufficient expertise safeguarded and
- The managed service providers must comply with the requirements stated in the outsourcing policy.
- Pension funds have enough countervailing power to manage the outsourced activities.
- Contractual service level agreements (SLA's) are made between the pension fund and the managed service provider containing detailed agreements regarding accountability reports, outsourced processes and key performance indicators to manage the outsourced activities.
- The pension fund must monitor the outsourcing relationship by obtaining reports regarding the outsourced activities, IT landscape and the functioning as a managed service provider as a whole periodically.
- Based on the SLA's and the obtained reports, the pension fund must evaluate the outsourcing polices and update if necessary.

3.4 The DNB Good Practice framework comparison

In the previous chapter, The DNB Good Practice Framework was explored. The following characteristics of the DNB Good Practice framework are identified:

- The Plan-Do-Check-Act cycle for continuous improvement.
- A maturity model.
- Information and cybersecurity controls categorised per organisational element.
- Origins from COBIT, NIST and the ISO 27000 family.

In order to ensure that the framework can increase the cyber resilience of pension funds, the framework will be compared to other frameworks. The different information and cybersecurity frameworks will be compared to each other and to which extend the characteristics of the framework corresponds with the characteristics of the DNB Good practice framework. Based on these analyses, the best framework is chosen for the comparison with the DNB Good Practice framework.

Relevant information and cybersecurity frameworks

There are various cybersecurity frameworks available consisting of standards, guidelines and best practices to help organizations to manage cybersecurity risks. In 2015 NOREA, the Dutch professional association for IT-auditors, has performed an analysis of several generally recognized cybersecurity standards and frameworks as part of drawing up and developing its Cyber Security Assessment methodology (CSA). This CSA methodology can be used as an instrument to help organizations get insight into cybersecurity risks. The CSA focuses on the assessment of the measures an organization can take to increase resilience within its IT environment.

For each standard/framework included in the analysis, an assessment was made for seven categories that are recognized within the Cyber Security Assessment (CSA). The seven categories within the Cyber Security Assessment of NOREA include:

1. Organization & Governance
2. Behaviour & Culture
3. Value chain (stakeholders) <-> Risks
4. Insight in the technological architecture (software, middleware, hardware)
5. Law & Regulations
6. Detection
7. Response

The following generally recognized cyber standards and frameworks have been analysed (NOREA, 2015):

Table 4: Information and cybersecurity frameworks investigated by NOREA

#	Creator	Framework
1	Information Security Forum (ISF)	Standard of the DNB Good Practice (SoGP) supplemented with Cyber Resilience Framework (CRF)
2	SANS Institute (SANS),	Critical Controls for Effective Cyber Defence (CCfECD)
3	Information Systems Audit and Control Association (ISACA)	Cybercrime Audit/Assurance Program
4	British Standards Institute (BSI)	PAS 555 Cybersecurity risk. Governance and management.
5	National Institute of Standards and Technology (NIST)	Cyber Security Framework
6	International Standards Organisation (ISO)	ISO27032 Guidelines for cybersecurity

The table below illustrates the results of the NOREA Cybersecurity assessment. The assessment is categorized based on seven categories and the score is labelled as follows:

- Red: The framework provides no guidance.
- Orange: The framework provides limited guidance
- Green: The framework provides good guidance.

Table 5: Results of the NOREA assessment per category

Categories	ISF - SoGP	SANS- CCfECD	ISACA – CAAP	BSI- PAS 555	NIST - CSF	ISO – ISO 27032
1. Organisation & Governance						
2. Behaviour & culture						
3. Value chain						
4. Insight into the technology						
5. Laws & regulations						
6. Detection						
7. Response						

In addition to the score, the following characteristics of pension funds are identified as important and will be weighted more heavily in the comparison between the frameworks:

- Value chain, due to the high percentage of outsourcing
- Insight into the technology, due to the sensitive data and large IT landscape.
- Laws and regulations, due to the legal obligations pension funds have.
- Detection and response, based on the IB monitor that stated that prevention is not enough, pension funds must shift to detection and response (DNB, 2020).

CCfECD, PAS 555 and the ISO/IEC 27032 frameworks provide no or limited guidance on the categories identified as important. The frameworks are examined, and they also miss parts or entirely characteristics of the DNB Good Practice framework, making them bad candidates for the comparison. The remaining frameworks: ISF SoGP, ISACA CAAP and the NIST CSF are further examined.

Information Security forum (ISF) - Standard of the DNB Good Practice (SoGP) supplemented with Cyber Resilience Framework (CRF)

The ISF has developed a standard of the DNB Good Practice (SoGP) for information security in which the measures necessary to maintain confidentiality, integrity and ensure availability of information. The practice is divided into the dimensions: governance, risk, compliance, people, process and technology. In addition to the Standard, the ISF has developed a Cyber Resilience Framework (CRF). This framework is intended to support organizations in the fight against cybercrime. The framework does not describe a ready-made set of measures to keep cybercrime at bay and guides organisation to anticipate and respond to security incidents resulting from cybercrime.

Table 6: The ISF framework assessed per category

Category	Score with substantiation
Organisation & Governance	Limited guidance provided; regarding governance of information and cybersecurity.
Behaviour & culture	Limited guidance provided; to the change of behaviour and awareness within the organization
Value chain	Good guidance regarding the value chain, assets are used as starting point
Insight into the technology	Limited guidance regarding the IT landscape of the organization, describes that hardware and software play a role, but is not main focus.
Laws & regulations	Good guidance provided
Detection	Good guidance provided
Response	Good guidance provided

Information Systems Audit and Control Association (ISACA) - Critical Controls for Effective Cyber Defence (CCfECD)

In 2012 ISACA developed a "cybercrime audit/assurance program" based on COBIT 4.1. The purpose of the program is to provide a single independent view of the measures to prevent cybercrime. The program emphasized that cybersecurity is not an IT issue, but an issue integrated into the entire business operations. This program consists of awareness, prevention, detection, incident management, crisis management and cooperation with the police and the judiciary in order to fight cybercrime. The program is primarily a summary and reorganization of COBIT standards related to information security and follow-up security incidents.

Table 7: ISACA framework assessed per category

Category	Score with substantiation
Organisation & Governance	Good guidance provided; organization must establish a cybercrime taskforce.
Behaviour & culture	Good guidance provided; awareness is emphasized as a crucial part.
Value chain	Limited guidance provided; primarily focusses on IT suppliers, not customers of the organization.
Insight into the technology	Good guidance provided; emphasis on the identification of the IT landscape
Laws & regulations	Good guidance provided
Detection	Good guidance provided; mainly technical, must have a taskforce
Response	Good guidance provided; must have a taskforce

National Institute of Standards and Technology (NIST) – Cyber Security framework

The NIST framework is based on different standards regarding information security, IT risk management and critical infrastructures like IS027001:2013, COBIT 5, CCS CSC, ISA 62443-2-1:2009, ISA 62443-3-3:2013 and NIST SP 800-53 Rev.4. The framework is written using an action-oriented approach that fits in with the plan-do-check-act cycle. This cycle is translated to the NIST approach with the activities: Identity, Protect, Detect, Respond and Recover. The model uses a capability maturity model through the implementation layers: 1. Partly, 2. Risk Aware, 3. Repeatable and 4. Adaptive. These layers reflect the maturity level of the organization of risk management process, integrated risk management program and external participation. This layered approach can be used for the continuous improvement of the organization. The area where the NIST model stands out is the detection and reaction areas. In detection, the NIST model focusses not only on threat intelligence but also corporation between organization regarding cybercrime. In the area of reaction (crisis management), NIST offers a practical guidance for managing cyber incidents and the recovery of incidents.

Table 8: NIST framework assessed per category

Category	Score with substantiation
Organisation & Governance	Good guidance provided; focus on processes, roles and responsibilities within the organisation
Behaviour & culture	Limited guidance provided; awareness is emphasized as a crucial part, but is mostly enforced by “tone at the top”
Value chain	Good guidance provided; all steps in framework are focused to protect the assets.
Insight into the technology	Good guidance provided; all steps of the framework are focused on the IT landscape.
Laws & regulations	Limited guidance provided; legal requirements are mentioned, but no substance is given.
Detection	Good guidance provided; emphasized by framework and incorporated into the framework’s core
Response	Good guidance provided; emphasized by framework and incorporated into the framework’s core

Comparison

By comparing the ISF, ISACA and NIST frameworks, the NIST framework came out the analysis as the most suitable framework for the comparison with the DNB Good Practice framework. The NIST framework scored the best on the seven categories when the weighted categories are taken into account. The NIST framework explicitly mentions the continuous improvement cycle and the maturity model as part of the framework, similar to the DNB Good Practice framework. The CCfECD framework required the establishment of a cybercrime taskforce and has limited guidance on the value chain. The value chain is very important for pension funds due to the high percentage of outsourcing, therefore the CCFeCD is not suitable as a framework for the comparison. The SoGP framework has limited attention to the IT landscape, which is very important for pension funds, since the sensitive participants data is located within the IT landscape. The limited focus on the IT landscape makes the SoGP not suitable for the comparison with the DNB Good Practice framework. In the following section, the NIST and the DNB Good Practice framework will be examined and compared on various levels.

Comparison NIST and the DNB Good Practice framework

The DNB Good Practice framework is from origin an information security framework. Cybersecurity is later added to this framework. To validate that the topics of information and cybersecurity are fully covered within this framework, a comparison is made with the NIST framework. The comparison is performed on the following three levels:

- High-level comparison.
  The high-level comparison compares the origin, approach, level of detail and the methods of both frameworks.
- Control-level comparison.
  The second comparison examines the controls of both frameworks. This is done by mapping the DNB Good Practice controls onto the different NIST control categories in order to find discrepancies. Also, trend reports will be examined to identify areas for improvement and check how the NIST framework handles these areas.
- Description-level comparison.
  In this comparison, the descriptions of the individual controls are compared to find discrepancies between controls.

High-level comparison:

A comparison has been made on four different high-level topics: Origin, approach, level of detail and method. In the table below these topics are compared.

Table 9: Comparison between the DNB Good Practice and the NIST framework

Level	The DNB Good Practice	NIST
Origin	Information security. In 2016, the focus shifted more to cybersecurity. Based on standards like COBIT, ISO 27000 family and NIST.	Based on best practices from (cyber)security frameworks like COBIT, ISO 27000 family, ISACA.
Approach	Organizational element approach, where all elements of pension funds are handled, more tailored for pension funds. Uses organizational elements to manage cybersecurity.	Cybersecurity activity approach uses cybersecurity activities to manage cybersecurity in organizational context.
Level of detail	Not a step-by-step implementation guide but explains the view of the supervisory authority of the correct interpretations of the laws and regulations. Gives more abstract controls, in order to let pension funds, choose what they prefer and reflect their nature and size.	Chronological implementation steps with a control catalogue with a more detailed description. Focused on cybersecurity.
Method	Describing controls related to its organizational elements, not chronological.	A chronological step-by-step high-level method with the activities: identify, protect, detect, respond and recover. With a focus of interlinking activities.

In the comparison of the two frameworks on a high level the following overlap was found: Both frameworks were based on international standards, make use of an interpretation of the Plan-Do-Check-Act cycle and both use maturity levels for assessments. The differences were the categorization of the controls, where the DNB Good Practice framework uses organisational elements to categorize its controls and the NIST framework uses chronological cybersecurity activities to categorise its controls. Also, the level of detail is different where the DNB Good Practice can be abstract in its controls; the NIST controls are more detailed and refer to an extra informative description. The high-level comparison of both frameworks gave insights into the similarities and differences of the frameworks, but a more in-depth comparison is needed in order to compare the frameworks effectively. In the following paragraph, the controls of both frameworks will be compared.

Control level comparison

An in-depth comparison of the controls of the frameworks is made. The first step is the comparison of the DNB Good Practice controls onto the activities of the NIST framework. The DNB Good Practice control is categorised in a NIST activity. This categorisation is done in two ways: where a DNB Good Practice control can overlap multiple NIST activities and where a DNB Good Practice control is dedicated to a single NIST activity. Simultaneously the trend reports are examined to find possible areas for improvement. The combination of the results of the comparison of controls and the examination of trend reports will lead to the in-depth analysis per control. The control analysis compares the description and implementation guidelines of the NIST controls and compares them with the controls of the DNB Good Practice framework. The complete analysis will lead to an in-depth comparison of both high and in-depth level between both frameworks. With the results of this analysis, the conclusion can be made if the DNB Good Practice framework is sufficient to manage cybersecurity for pension funds and if it contains all the requirements from the perspective of a dedicated cybersecurity framework.

Mapping of the controls

The 58 DNB Good Practice controls have been examined and mapped on the five activities of the NIST framework. The activities are identify, protect, detect, respond and recover. Per control is checked under which activity the control can be categorised. The categorisation is made in two different ways: the first way is where a control can be categorised in multiple NIST activities and the second one is where a control is dedicated to one NIST activity.

The first diagram shows the controls of the DNB Good Practice mapped into the NIST activities where a single DNB Good Practice control can be categorised in multiple NIST activities.

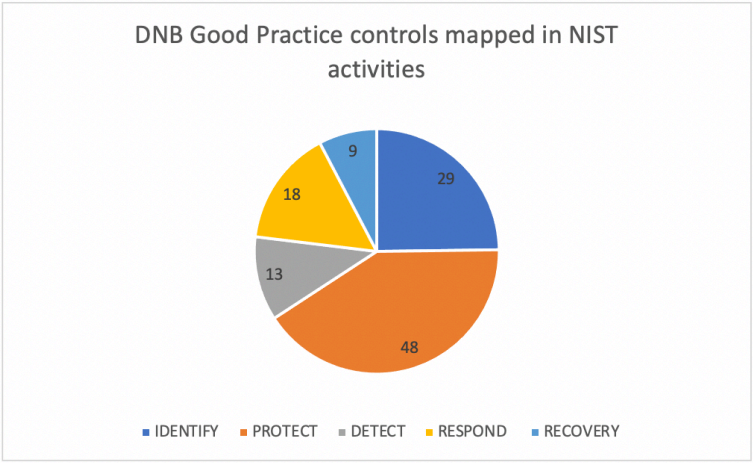

Figure 9: The DNB Good Practice controls mapped in the 5 NIST activities where controls can be mapped in multiple NIST activities

In the second diagram, the DNB Good Practice controls can be categorised in only one NIST activity. An interesting observation here is that the NIST activities respond and recovery only have a combined total of 4 dedicated controls.

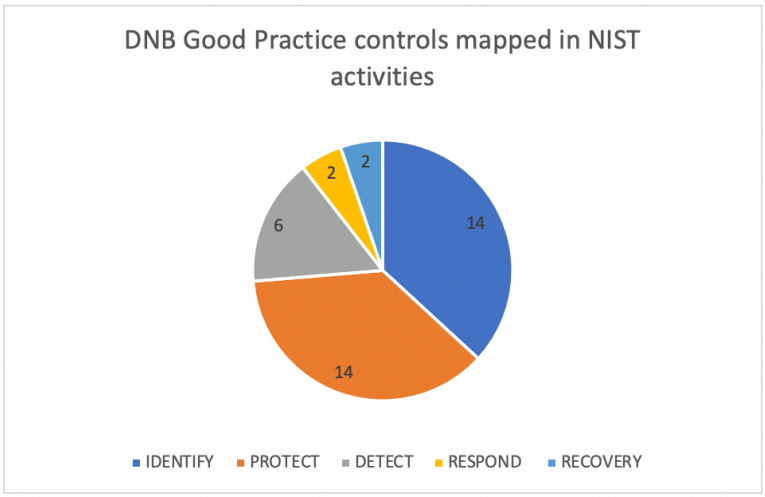

Figure 10: The DNB Good Practice controls mapped in the 5 NIST activities where controls cannot be mapped in multiple NIST activities where some DNB Good Practice controls are not mapped into the NIST activities.

The last diagram shows how the NIST framework has categorised its controls.

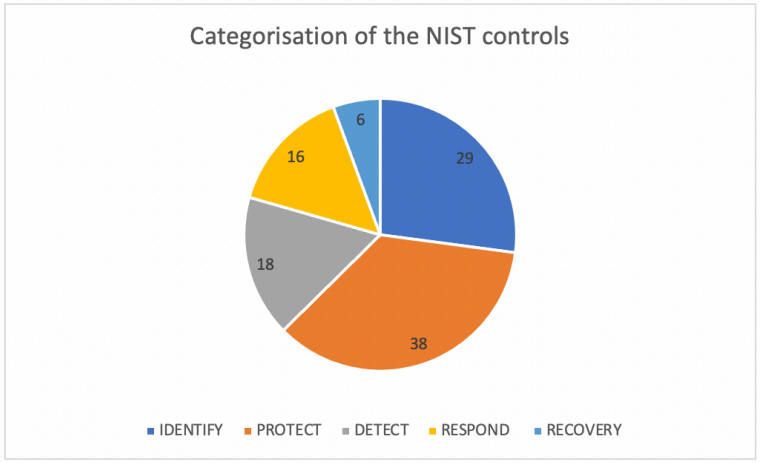

Figure 11: Categorisation of the NIST controls per NIST activity

Comparing the amount of the DNB Good Practice controls to the NIST activity recover and respond shows that the DNB Good Practice only has 2 dedicated controls for recover and respond, while NIST has 16 controls for respond and 6 for recovery.

The mapping of the DNB Good Practice controls within the NIST framework showed that the NIST framework places more emphasis on the categories response and recovery. Subsequentely,the IB monitor states that pension funds must focus more on the detection and reponse regarding to information and cybersecurity (DNB, 2020). In the following section, the content of the controls is compared to examine if the DNB Good Practice misses controls, especially regarding the categories response and recovery.

Description level comparison

In the last comparison between the NIST and the DNB Good Practice framework, the content of the controls is compared. The comparison is made by listing the NIST controls in combination with the extra informative references and then check if the content of the DNB Good Practice controls covers the content of the NIST control. The combination with the informative references is done since some NIST controls are summarized and not comprise all content stated in the informative reference where the control is based upon.

The following findings have been made in the content comparison of controls. The DNB Good Practice model scores low on parts of the following controls:

- Contingency controls
- Incident response controls
- Vulnerability training controls
- Awareness and training controls.

Contingency controls

The DNB Good Practice scores low on the controls CP-2 and CP-3.

- CP-2: Coordinates contingency planning activities with incident handling activities.
- CP-3: The organization provides periodic contingency training to information system users consistent with assigned roles and responsibilities. This contingency training incorporates simulated events to facilitate effective response by personnel in crises.

The DNB Good Practice scores low on this control because the DNB Good Practice has no control that incorporates simulated events for contingency training.

Incident response controls

The DNB Good Practice scores low on IR2 and IR3.

- IR2: The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crises.
- IR3: The organization periodically tests the incident response capability for the information system using to determine the incident response effectiveness and documents the results.

The DNB Good Practice framework scores low on these controls because the DNB Good Practice has no control that incorporates simulated events for response training.

Vulnerability controls

The DNB Good Practices scores low on CA-8.

- The organization employs information and cybersecurity exercises to simulate attempts by adversaries to compromise organizational information systems.

The DNB Good Practice framework scores low on this control. The scenario-based testing is named once and is given little emphasis by the framework.

Awareness and training controls:

The DNB Good Practice score low on the NIST controls: AT3 and AT4

- AT3: The organization provides role-based security training to personnel with assigned security roles and responsibilities where the organisation includes practical exercises in security training that reinforce training objectives. In addition, the organization provides training to its personnel on how to recognize suspicious communications and anomalous behaviour in organizational information systems.
- AT4: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training and retains individual training records.

The DNB Good practice framework scores low on this control. Role based and simulated based security training is mentioned within the DNB Good Practice framework but with little emphasis. This also applies to documenting and monitoring of the awareness and training exercises of pension fund board members.

The description comparison was focussed on the topics of detection and response. In this comparison, the description of the individual controls was compared to find discrepancies between the controls. The difference between the NIST controls and the DNB Good Practice framework controls was that the NIST controls are more descriptive and give more insight into the implementation of controls. In the DNB Good Practice Framework, the controls are more abstract and do not provide such handles. The DNB Good Practice Framework missed or scored low on the parts of the following controls:

- Contingency controls: CP-3, This control emphasised that the organisation provides contingency training to employees with assigned roles and responsibilities where simulated events are incorporated. This is done to facilitate effective response by personnel in crises.
- Incident response controls: IR2 and IR3, these controls emphasise the incorporation of simulated events into incident response training.
- Vulnerability controls: CA-8, this control emphasises red team exercises to stimulate recognising attempts by adversaries to compromise organisational information systems in accordance with organisation defined rules of engagement.
- Awareness and training controls: AT3 and AT4 emphasise that the organisation provides role-based security training to personnel and documents and monitor individual security training activities.

3.5 Conclusion

Chapter 3 concerned the review of the governance frameworks. This chapter primarily focusses on finding the required state of pension funds regarding information and cybersecurity. The overarching aspects of managing information and cybersecurity are the laws and regulation applicable to pension funds. These laws and regulation form the scope in which pension funds operate.

As a result of the document review, three main topics arose that contributed to information and cybersecurity in pension funds in order to comply with the laws and regulations. For these three topics, the required state is identified. The three identified topics are:

1. The DNB Good Practice framework
2. Knowledge, experience and countervailing power
3. Governance domains.

Laws and regulations

The following laws and regulation have been identified that describe on a high level the required state for pension funds managing information and cybersecurity.

- Article 143 of the pension act states that pension funds organize their pension fund in such a way that controlled and sound business operations are safeguarded.
- Article 34 of the pension act states that pension funds are permitted to use outsourcing, but they remain ultimately responsible, must have contractual agreements and have enough countervailing power (knowledge and experience) safeguarded within the fund to be in control of the outsourced activities.
- Article 3.17 of the financial supervision act states that financial institutions must have adequate procedures and measures in place to control IT risks. Also, DNB emphasizes the importance of the alignment between business and IT.
- Policy rule 2012 on suitability states the requirements for pension fund board members.

Knowledge, experience and countervailing power

Policy rule 2012 on suitability states the different requirements of pension fund board members. Examination of the policy showed no hard IT requirements regarding knowledge or experience for pension fund board members is incorporated. Although, as stated in Article 34 of the pension act, it is expected that pension funds have enough countervailing power safeguarded within the board to be in control over their outsourced activities. The required state of pension funds regarding knowledge, experience and countervailing power is that a pension fund has safeguarded IT knowledge and experience and thus countervailing power within their fund for managing their outsourced IT processes.

Governance domains

To help pension funds with the compliance of article 143 and 34 of the pension act that safeguard sound and controlled business operations, DNB made various guidance documents. The guidance documents provided practical substance to the following domains:

- Outsourcing
- Integrated risk management
- IT.

These three governance domains form the base for managing the IT function, information and cybersecurity. Also, the governance domains contribute to the alignment between the business demands of the pension funds and the IT supply of the managed service provider. The required state of pension funds regarding the governance domains is that the pension fund has correctly implemented the governance domains, they are aligned, and they contribute to the alignment between the business and IT. This ultimately contributes to the solid IT foundation whereby information and cybersecurity can be implemented.

The DNB Good Practice framework

DNB has made the DNB Good Practice framework to provide a practical interpretation of laws and regulations regarding information and cybersecurity. The framework has been compared to the NIST framework to check if all the information and cybersecurity aspects are covered. The comparison showed that the DNB Good Practice framework is well-tailored for managing information and cybersecurity but falls short on certain aspects compared to the NIST framework in relation to cybersecurity. The DNB Good Practice framework has less emphasis on respond and recovery aspects and scores low on the following controls:

- Contingency controls
- Incident response controls
- Vulnerability training controls
- Awareness and training controls.

The DNB Good Practice provides insufficient substance for the implementation of these control while the NIST framework is very descriptive and places a lot of emphasis on these aspects. The required state for pension funds regarding the DNB Good Practice framework is that pension funds have implemented the framework and pay extra attention to the aspects where the DNB Good Practice falls short.

Chapter 4: Survey design and analysis

This chapter concerns the main analysis of the research. The following section explains how the analysis was performed and the consecutive chapter describes the results of the analysis.

4.1 Survey design

In chapter 3: Review of the governance frameworks, three topics were identified as the most important topics that contribute to the state of information and cybersecurity for pension funds. The survey is based on the topics of the DNB Good Practice framework in combination with the identified NIST topics the DNB Good Practice scored low on. The following topics were identified:

1. The DNB Good Practice framework
2. Knowledge, experience and countervailing power
3. Governance domains.

A survey has been designed to provide insight regarding the current state of the identified topics within Dutch pension funds. The survey was distributed between September and October. A total of 54 pension funds were approached for the survey and 25 pension funds filled out the survey, making the response rate of the survey 46%.

The three main topics were divided into smaller related subtopics and for each of these subtopics' questions were asked in the survey. This provided substance to the main topic and made it possible to understand the rationale of the pension fund. The results of the analysis of the survey were validated by a total of 3 pension fund board members and is validated with one of the creators of the DNB Good Practice framework.

The comprehensive survey design and results of the survey are listed in appendix B.

4.2 Analysis approach

The three identified topics, as described above, are divided into smaller related topics for a thorough analysis. A gap analysis is performed on each of the smaller topics. The results of the gap analyses provide valuable input for the needed improvement of the current state of information and cybersecurity for pension funds.

The gap analysis consists of five steps and is linked to the sub-questions of this research. By conducting the gap analysis, the sub-questions can be answered, which ultimately contributes to answering the main research question. The figure below provides a schematical overview of the different steps of the gap analysis.

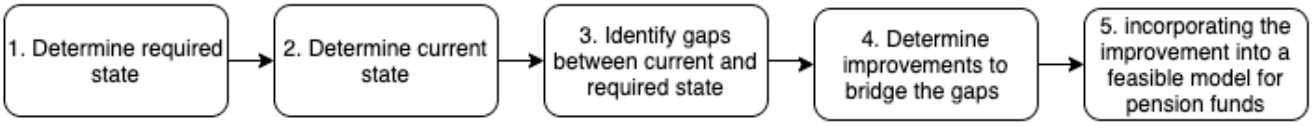

Figure 12. The schematic overview of the GAP analysis used in this research.

4.3 The DNB Good Practice framework

The DNB Good Practice framework is a practical interpretation of the laws and regulations for pension funds for managing information and cybersecurity. By complying and implementing the DNB Good Practice framework, pension funds safeguard sound and controlled business operations. In chapter 5, the required state is described regarding the DNB Good Practice framework and the underlying laws and regulations. In the following section, gap analyses are performed regarding the smaller related topics to the DNB Good Practice framework. The following topics are covered:

1. Adoption of the DNB Good Practice framework
2. Scenario-based testing and training
3. Pension fund ISAC
4. IT landscape
5. Accountability reports

4.3.1 Adoption of the DNB Good Practice framework

Current state 1: The adoption rate of the DNB Good Practice framework is low

The results of the survey provide insight into the adoption rate of the DNB Good Practice framework. The adoption of the DNB Good Practice framework includes the implementation of the controls and the risk management cycle of the framework. Of the responding pension funds, 61% have not adopted the DNB Good Practice framework.

The results show that pension funds approached by DNB for the theme-oriented study of information and cybersecurity have a higher adoption rate (57%) compared to pension funds not approached by DNB (12,5%). A strong correlation is visible between the supervision of DNB and the adoption of the DNB Good Practice.

It is more common that larger pension (T3, T4) funds have adopted the DNB Good Practice framework than smaller funds (T2, T1). A possible explanation for this could be that the adoption rate of the DNB Good Practice framework is driven by the supervisory authority. DNB primarily focusses on T2 or larger pension funds and increases the scope and depth of the supervision based on the size of the fund (DNB, 2012). The supervision of DNB could increase the awareness and importance of information and cybersecurity among board members, which could result in that information and cybersecurity gets more attention within the pension fund agenda.

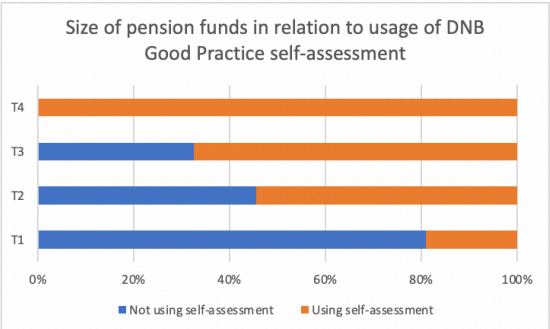

Figure 13. Sizes of pension funds expressed in the T-classes concerning the usage of the DNB Good Practice self-assessment displayed in percentage.

Gap 1: The adoption rate of the DNB Good Practice framework within pension funds is insufficient.
The DNB Good Practice framework provides pension funds with a practical interpretation of laws and regulations regarding information and cybersecurity. The DNB Good Practice framework is not enforced but is highly recommended by DNB. The required state is that all pension funds have implemented the DNB Good Practice framework for effectively managing information and cybersecurity. By comparing the current state to the required state, the following gap can be identified: The adoption rate of the DNB Good Practice framework within pension funds is insufficient.
Improvement 1: Creating awareness of information and cybersecurity within the pension fund board to increase the adoption rate of the DNB Good Practice framework.
The goal of this improvement is to intrinsically motivate pension fund board members to use the DNB Good Practice framework. This can be achieved by increasing the awareness and knowledge regarding information and cybersecurity among pension fund board members. To intrinsically motive pension fund board members to understand the importance of information and cybersecurity the following aspects are needed: • Knowledge • Awareness and training • Continuous approach In order to provide substance to this improvement, a continuous improvement model is developed, which will be further elaborated in chapter 5 The improvement model contains various activities that focus on increasing the knowledge and awareness of pension fund board members.
Validation
The results have been validated with some pension fund board members and DNB. DNB indicates that the usage of the DNB Good Practice framework and self-assessment is primarily used when the DNB announced their supervision of the fund. They acknowledge that it is common that pension fund board members have less intrinsic motivation to implement the DNB Good Practice framework, partly because of the complicated subject, and partly because they lack the knowledge and expertise to implement this. This is in line with the response of the pension fund who responded for the validation. The pension fund board members indicated that due to the outsourcing, information and cybersecurity receives less attention. They find the topic of information and cybersecurity difficult, since they have little expertise and knowledge regarding the subject. The combination of the outsourcing and the little expertise and knowledge leads to less attention from the pension fund board. Only when the DNB announce their visit, they are required to look at the DNB Good Practice framework. The usage of the DNB Good Practice framework is driven by the supervisory authority and not from within the fund.

4.3.2 Scenario-based testing and training

Current state 2: Scenario-based testing and training is insufficiently utilized by pension funds and in combination with their managed service providers.

The results show that 96% of the responding funds do not use scenario-based incident response or business continuity training or testing. Also, only 18% of the responding pension fund uses cooperative testing with their managed service providers.

The current state shows that: Scenario-based testing and training are insufficiently utilized by pension funds and in combination with their managed service providers.

Gap 2: Scenario-based testing and training in the pension funds and cooperation with the managed service providers is insufficient.

This comparison between the DNB Good Practice and the NIST framework showed that NIST places more emphasis on scenario-based testing and training, especially in the fields of incident response and business continuity. Both frameworks emphasize on the cooperation with managed service providers. These topics together form the required state of pension funds: Pension funds must incorporate scenario-based testing and training within the pension funds and in cooperation with their managed service providers.

The current state shows that almost none of the pension funds use scenario-based testing and training in the fields of incident response and business continuity. Also, a low percentage of responding pension funds cooperate with their managed service providers for information and cybersecurity testing and training.

By comparing the current state to the required state, the following gap can be identified: Scenario-based testing and training in the pension funds and the outsourcing chain is insufficiently incorporated. This gap can additionally be substantiated with the results of the DNB information security monitor of 2020 (DNB, 2020).

Improvement 2: Improving the usage of scenario-based testing and training within the fund and in the outsourcing chain.

Scenario-based testing and training must be incorporated within the awareness and training plan of pension funds. Emphasis should be placed on cooperative scenario testing with managed service providers. The pension fund board and personnel must actively participate in the training to increase effective response in crises and to increase their awareness. The scenario-based training should be based on current information and cybersecurity risks or based on risks identified in the IT risk assessment. The result of the testing and training exercise should be documented, monitored and evaluated.

Validation

The usage of scenario-based testing and training is validated among pension fund board members and DNB. Pension fund board members don't find scenario-based testing necessary if information and cybersecurity is already properly managed by their managed service provider. Pension fund board members think that their managed service providers do not have the time for cooperative scenario-based testing and training and are therefore more likely to rely on accountability reports.
DNB states that the use of cooperative scenario-based testing and training is an excellent tool to improve the awareness, knowledge and the outsourcing relationship with their managed service providers.

4.3.3 Pension fund ISAC

Current state 3: Pension funds are not affiliated with the pension fund ISAC.

The results of the survey provide insight regarding the affiliation of pension funds with the pension fund ISAC. The results show that none of the responding pension funds is affiliated with the pension funds ISAC.

After further examination of the pension fund ISAC, it appears that that only self-administering pension funds and pension fund administrations can be affiliated (De Nederlandsche Bank, 2018). The non-administrative pension funds may not be affiliated according to DNB, although the DNB Good Practice state that they must be affiliated. Also, the pension fund ISAC is primarily focused on the IT domain pension administration, not including the board environment domain and the asset management domain.

Gap 3: The current pension funds ISAC is not sufficient enough for pension funds.

The DNB Good Practice framework states that pension fund must have threat intelligence in place and that this can be achieved by the affiliation with the pension fund ISAC. Therefore, the required state is that pension funds must be affiliated with the pension fund ISAC. By comparing the current state to the required state, the following gap can be identified: The current pension fund ISAC is not sufficient enough for pension funds.

Improvement 3: Improving the threat intelligence and impact analysis for pension funds.

Pension funds must obtain relevant information and cybersecurity updates and development from all the IT domains they are associated with. If new risks of threats are identified based on the threat intelligence, pension funds must incorporate this into their IT risk framework. Newly identified threats or risks could be used for scenario-based training and testing, which helps to increase the pension fund's information and cybersecurity awareness and resilience.

In order to achieve this, a sector threat intelligence must be established for pension funds for the IT domains of asset management and for pension administration. The IT domain board environment must have a proactive stance regarding information and cybersecurity threats since their IT infrastructure is more general. In order to obtain this threat intelligence pension funds can cooperatively setup an ISAC or be affiliated with an existing one. The branch organisation could possible help pension funds with setting up this ISAC. However, it is important that the pension fund itself gives substance to this and does not let it depend on the supervisory authority.

Validation

The usage of the pension fund ISAC training is validated among pension fund board members and DNB. Some pension funds didn't know the pension fund ISAC existed. Some pension fund didn't find it necessary since they outsourced all information and cybersecurity activities and receive periodic accountability reports from their managed service providers.

DNB indicates that the ISAC can be best tackled from the sector rather than from the supervisory authority. The reason behind this idea to improve the intrinsic motivation of pension fund board and if DNB enforces it, it becomes a requirement where pension funds must comply to. DNB sees that pension funds do not cooperate very well compared to other financial institution and that this could help to improve to improve the information and cybersecurity stance of the fund.

It is important that the pension fund pension obtain information regarding information and cybersecurity from multiple channels. Every channel has a different angle of approach and can increase the awareness of the board members.

4.3.4 IT landscape

Current state 4: Pension funds have insufficient insight and overview regarding their outsourced IT landscape.

The results of the survey provided insight into the overview of the IT landscape pension funds obtain from their managed service providers. The IT landscape includes the used applications per outsourced service, critical outsourced services and location of stored data. The identification of the IT landscape is crucial for effectively assessing IT risks.
The results show that a low percentage of pension funds obtains an overview of their IT landscape from their managed service providers. 64% of the pension funds obtain this overview from their pension administration, 50% of the board environment and only 36% of the asset management domain.

Half of the responding pension funds do not have an overview of their IT landscape, making it hard to monitor and manage information and cybersecurity risks. Having this overview is one of the prerequisites for having enough countervailing power for managing the outsourcing relationship. By not having this overview pension funds do not know where the personal data of their participants is located and how it is protected. The location of the personal data of the participants of the fund is very important due to laws and regulation, like the GDPR, regarding personal data.

Gap 4: A low percentage of pension funds have an overview of their IT landscape

Laws and regulation require the pension funds to have adequate procedures and measures implemented to manage IT risks, have enough countervailing power to manage the outsourcing relationship and must have controlled and sound business operations. This begins by having an overview of the IT landscape. Therefore, the required state of pension funds is that all pension funds have an overview of their IT landscape.

By comparing the current state to the required state, the following gap can be identified: Pension funds have insufficient insight and overview regarding their IT landscape.

Improvement 4: Increasing the percentage of pension funds that obtain the overview of their IT landscape

The percentage of pension funds that obtain an overview of their IT landscape must be increased. Pension funds must make arrangements with managed service providers that the pension fund periodically obtains an overview of IT landscape, including the used applications per outsourced service, critical outsourced services and location of stored data. Pension fund must obtain this for their managed service providers of all their IT domains. Also, the contractual agreement must include that the pension fund will be notified if changes occur in the IT landscape of the managed service provider.

Validation

The overview of the IT landscape is validated among pension fund board members. Pension fund are not actively mapping out their IT landscape and obtain this mainly on the basis of accountability reports that are periodically provided. The pension funds are not sure whether the entire IT chain, including systems, application, third parties and locations of data are mapped. The pension fund overview is based too much on trust, and because of the lack of knowledge, the assumption that the accountability reports provided are sufficient.

4.3.5: Accountability reports

Current state 5: Pension funds receive a low percentage of accountability reports regarding information and cybersecurity from their managed service provider.

The results of the survey show that the number of accountability reports obtained by pension funds from their managed service providers are low, especially regarding information and cybersecurity.

A distinction is made between pension funds who use the DNB Good Practice framework and pension funds who do not use it. Although pension funds who use the framework scored higher than the pension funds who do not use it, it still shows that the percentage of accountability reports obtained regarding information and cybersecurity is low. The reports with a strong focus on information and cybersecurity (ISO 27001, Cyber maturity, Incident reports with cyber incidents and the results of the DNB Good Practice self-assessment) are insufficiently obtained by pension funds, especially by pension funds who do not use the DNB Good Practice framework.

Assurance reports	USING GP:SA	Not using GP	All
SLR-report	52%	64%	59%
NFR-report / Risk report	63%	56%	59%
ISAE 3402	93%	90%	91%
ISAE 3000 (SCO2 report)	22%	33%	29%
ISO 27001	26%	8%	15%
Cyber maturity report	26%	5%	14%
Incident reports with cyber incidents	63%	49%	55%
Results Good Practice self-assessment	67%	26%	42%

Figure 14: Accountability reports obtained from managed service providers in percentage. A comparison is made between pension funds who use the DNB Good Practice self-assessment and pension funds who do not use it (GP stands for the DNB Good Practice)

Gap 5: A low percentage of pension funds obtain accountability reports regarding the topics of information and cybersecurity with the correct scope and depth.

Laws and regulations state that pension funds must safeguard enough countervailing power within the board to be in control over their outsourced activities. The DNB Good Practice framework places a lot of emphasis on obtaining and reviewing accountability reports from the pension funds managed service providers. The accountability reports enable the pension fund to monitor, analyse and adjust the outsourced activities. The required state of pension funds is to have sufficient countervailing power safeguarded within the board to manage the outsourcing relationship. This can be achieved by obtaining and reviewing accountability reports regarding information and cybersecurity to monitor, manage and adjust the outsourced processes and activities.
By comparing the current state to the required state, the following gap can be identified: A low percentage of pension funds obtains accountability reports regarding information and cybersecurity.

Improvement 5: Improving the correct usage of accountability reports with the correct scope and depth.

Pension funds must make agreements with their managed service provider for the different IT domains regarding accountability reports. The pension fund must ensure that the managed service provider provides sufficient evidence to monitor and manage the outsourced activities. Pension funds must ensure that sufficient evidence is provided to

evaluate the effectiveness of the implemented controls proportionally and that this is recorded within the contractual agreements between the pension fund and the managed service provider. The contractual agreements must be periodically monitored and evaluated to ensure that pension fund obtains evidence with the correct depth and scope to monitor and manage their information and cybersecurity.

Validation

The topic of accountability reports obtained is validated among pension fund board members. It emerged that pension fund are not pro-active in obtaining the accountability reports and trust that their managed service provider has information and cybersecurity properly arranged. Pension funds are not very inclined to ask for specific accountability aspects, because the lack of knowledge of the subject and pension funds have the idea that they "bother" their managed service provider with these requests since they administer multiple pension funds.

4.3.6 Summary: The DNB Good Practice framework

Pension funds do not adequately implement the DNB Good Practice framework

Based on the different sub-states as mentioned above, the general state can be determined regarding the adoption of the DNB Good Practice framework.

Pension funds fall short when it comes to the adoption of the DNB Good Practice framework, the self-assessment and the associated controls. The adoption rate of the DNB Good Practice self-assessment is low and the pension funds who use it, do not fully implement the controls. The pension funds score low on the following aspects:

- The adoption rate of the DNB Good Practice self-assessment is lo
- Scenario-based testing
- The affiliation with the pension funds ISA
- Overview of their outsourced IT landscape;
- The percentage of accountability reports obtained regarding information and cybersecurity;

Based on the results of the responding pension, the following conclusion can be drawn: The adoption rate of the DNB Good Practice framework is insufficient and the controls within the framework are not fully implemented.

Pension funds find it difficult to take control of their outsourced information and cybersecurity activities and processes. The pension funds trust their managed service providers that they have their information and cybersecurity properly arranged. Managing information and cybersecurity is not the top priority of the pension fund because it is outsourced and presumably well-arranged and there is insufficient knowledge and awareness amongst pension fund board members.

4.4 Knowledge, experience and countervailing power

The required state according to laws and regulation describes that pension funds must have countervailing power safeguarded within the fund. In addition, the pension fund must have adequate procedures and measures to manage IT risks. These laws and regulation require that pension fund board members must have knowledge and experience regarding IT to have enough countervailing power and to effectively manage IT risks. In the following section the gap analyses are performed regarding the divided related topics to the suitability plans. The following topics are covered:

1. IT requirements in suitability plans
2. IT knowledge and experience within the pension fund board

4.4.1 IT requirements in suitability plans.

Current state 6: A low percentage of pension funds has IT requirements for pension fund board members incorporated in their suitability plans.

The results of the survey provided insight into the subject of IT requirements in suitability plans for pension funds. The results of the survey showed that 95% of the responding pension funds has a suitability plan where the requirements regarding knowledge and experience are described. Of this percentage, 43% of the pension funds also included knowledge and experience requirement regarding IT. This shows that the majority has not incorporated IT requirements in their suitability plans.

Gap 6: A low percentage of pension funds has IT requirements for pension fund board members incorporated in their suitability plans.

There are no hard requirements stated in laws and regulation regarding the incorporation of IT in the suitability plans for pension fund board members. Although in the DNB Good Practice it is stated that basic IT knowledge regarding information and cybersecurity is safeguarded within the fund. The topic of IT is increasingly becoming more important for pension fund and therefore should be a requirement in the suitability plans and even in the policy rule in suitability 2012. The missing of the IT requirements in the suitability plans of pension funds can be identified as a gap.

Improvement 6: Adoption of IT requirements in the suitability plans of the pension fund

Pension funds must incorporate IT requirements, including relevant IT work experience and IT knowledge, in their suitability plans. In order to safeguard IT knowledge within the pension fund, there needs to be a development plan for the pension fund board in order to keep their IT knowledge up to date. The development plan can be incorporated in the awareness and training plan and must be periodically monitored and evaluated.

Validation

The topic of a suitability plan is validated among pension fund board members and DNB. Pension funds that have not incorporated IT requirements state that they are aware of this and that its due to the size of the fund. They safeguard the IT expertise by making someone within the board accountable for it and he calls in experts when the fund is faced with information and cybersecurity issues. Other pension funds indicate that they are working on this based on the requirements stated in the DNB Good Practice framework but have not yet incorporated IT requirements in their suitability plans.

DNB states that the missing of the hard IT requirements is useful to them because they can give more substance to this subject via their open standard supervision. DNB is working with parties that provide training for pension fund board members to incorporate IT in their compulsory curriculum.

4.4.2 IT knowledge and experience within the pension fund board.

Current state 7: IT knowledge and experience are insufficient safeguarded within the board of the pension fund and among the different IT domains

The results of the survey provided insight into the professional IT knowledge and IT work experience among the different IT domains. Professional knowledge is defined in the survey as "global IT-related knowledge concerning the risks, processes and systems of the primary processes of a pension fund". Work experience was defined as two years of work experience, of which at least one consecutive year in a relevant work environment.
The result is that 59% of the responding pension funds have knowledge and experience regarding IT safeguarded within the board. The knowledge and experience are mainly located within the IT domain pension administration with 47%, within the board environment with 32% and less located within the asset management domain with 18%.
A potential explanation regarding the high percentage of knowledge located within the IT domain of pension administration could be that DNB primarily emphases on the outsourcing relationship between the pension fund and pension administration. The asset management domain falls under the supervision of the AFM, who have a different approach of supervision. In addition, it is common the asset managers are international organisation where international rules apply.

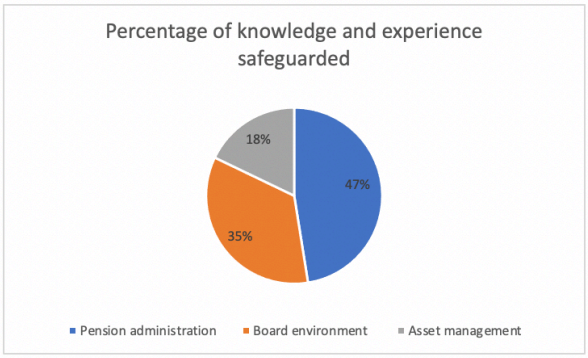

Figure 15: Distribution of knowledge and experience among the different IT domains.

Gap 7: There is insufficient IT experience and knowledge safeguarded within the pension fund board.

The required state of knowledge and experience is based upon the requirements made for policymakers of section B of the policy rule suitability 2012. These requirements are (in addition to existing requirements):

- General and specific professional IT knowledge gained in a relevant work environment in regard to business operations.
- Where specific professional knowledge has been acquired at least two years of work experience of which at least one consecutive year.
- Requirements are proportionate to the scope, scale, nature and complexity of the activities of the pension fund.

The results of the survey show that 59% of the responding funds have safeguarded IT knowledge and experience within their pension fund. Of this percentage, the majority of the knowledge and experience is located within the pension administration domain. This shows that 41% of the responding pension funds have no basic knowledge and experience regarding IT safeguarded within their board. The IT knowledge and experience that is present within the pension fund board is mainly located to the pension administration, where DNB places a lot of emphasis on. By comparing the current state to the devised required state, the

following gap can be identified: There is insufficient IT experience and knowledge safeguarded within the pension fund board.

Improvement 7: Increasing the level of IT knowledge among pension fund board members regarding the IT and the outsourced IT domains.

The level of IT knowledge among pension fund board members must be increased. This must be increased on a general level and more specified for each of the IT domains. Periodically pension fund board members must have educational sessions with their managed service providers to increase their knowledge regarding the IT topics of the managed service provider. These educational sessions must also include topics regarding information and cybersecurity. This must all be documented for the monitoring and the evaluation of the educational progress of the board members.

In addition, to increase the level of knowledge regarding the different IT domains, the pension fund can be affiliated with a pension fund ISAC. The pension fund ISAC informs the pension fund about new development regarding all IT domains, helping pension fund board members to ask more critical questions by their managed service providers.

Validation

The topic of IT knowledge is validated among pension fund board members and DNB. Pension fund board members are busy increasing their knowledge through educational seminars, but due to the size and complexity of the subject, it is difficult for board members to comprehend the subject. Pension funds are aware of the lack of knowledge and request ad-hoc expertise when the fund is faces IT related issues.

DNB states that the knowledge among pension fund board members is increasing, but they are not a fully-fledged discussion partner when it comes to IT. They aim to improve this by incorporating IT at institutions that educate pension fund board members.

4.4.3 Summary: Knowledge and experience

General current state: There is too little knowledge and experience safeguarded within the pension fund board for effectively managing the (outsourced) IT processes, especially regarding information and cybersecurity.

Less than half of the responding pension funds have incorporated IT requirements in their suitability plans. This reflects in the fact that 41% of the responding pension funds have IT knowledge or experience safeguarded within the board of their pension fund. The 59% that has safeguarded IT knowledge and experience is mainly located in the IT domain of pension administration. Pension fund board members are not yet at the level to be fully-fledged discussion partners when it comes to IT, but their level of knowledge is increasing.

As stated in gap 4, a low percentage of pension funds obtain an overview regarding the IT landscape of the IT domain. Gap 5 stated that there is a low percentage of pension funds that receive the correct accountability reports regarding their outsourced processes and activities. By combining this information with the little knowledge and experience safeguarded within the pension fund, the following conclusion can be drawn: Pension funds have insufficient knowledge and experience safeguarded within the board of pension fund to effectively manage the (outsourced) IT processes.

4.5 Governance domains

Laws and regulations state that pension funds must safeguard sound and controlled business operations. In order to help pension funds to comply with these laws and regulations, DNB created various guidance document that provided practical substance regarding the governance domains to comply with laws and regulations. DNB created guidance documents for the following governance domains:

- Outsourcing
- Integrated risk management
- IT.

These aspects are reflected in the IT Governance alignment model. This model describes how pension funds can give substance for managing their IT function by incorporating all the governance aspects. The domains described in the model, form the basic governance domains that pension funds must meet in order to be in control of their IT function. These domains also form the basis for the pension fund to properly implement information and cybersecurity. The required state of pension funds is that all the domains are fully implemented and aligned. In the following section, the gap analyses are performed regarding the smaller related topics of the guidance documents. The following topics are covered:

1. DNB guidance documents
2. Alignment between the governance aspects
3. IT risk appetite.

4.5.1 DNB guidance documents
Current state 8: Not all pension funds have an IT policy
The results of the survey provided insight into the usage of the incorporation of different guidance documents within the pension funds. The results show that all responding pension funds have an outsourcing policy document that gives substance to the governance aspects of outsourcing. This also applies to the governance aspects of IRM. IT policy is the only governance aspects that not all pension funds have incorporated; 18% of the pension funds don't have an IT policy.
Gap 8: Not all pension funds have an IT policy
The required state of pension funds regarding the integration of DNB governance aspects it that all governance aspects must be integrated to form a base for managing IT. By comparing the current state to the required state, the following gap can be identified: Not all pension funds have an IT policy.
Improvement 8: Drafting of the IT policy.
Pension funds must have an IT policy which describes how the pension funds manage the IT function. The IT policy will be incorporated into the improvement model and is a prerequisite in order to use the model.
Validation
The topic of IT knowledge is validated among pension fund board members. Pension funds have drafted an IT policy; however, it emerged that some pension funds paid little attention to it. The IT policy was generally not aligned with other governance domains. The management of IT and thus the IT policy do not have a high priority on the pension fund board agenda.

4.5.2 Alignment between governance domains

Current state 9: The alignment between the governance aspects can be improved

The results of the survey provided insight into the alignment between the governance aspects IT policy and the outsourcing policy, IRM policy and the pension fund strategy. The pension funds were asked to score their alignment with a 4-point based Likert-scale where 1 is not aligned and 4 is fully aligned. The results show that the alignment between the different governance aspects is divided, see figure 12. The majority (63%) of the pension funds have aligned their IRM with their IT policy. Half (50%) of the pension funds have aligned their outsourcing with their IT policy and 36% has aligned their strategy with their IT policy. The alignment between the governance domains can be improved, especially the alignment between the IT policy and the strategy of the pension fund.

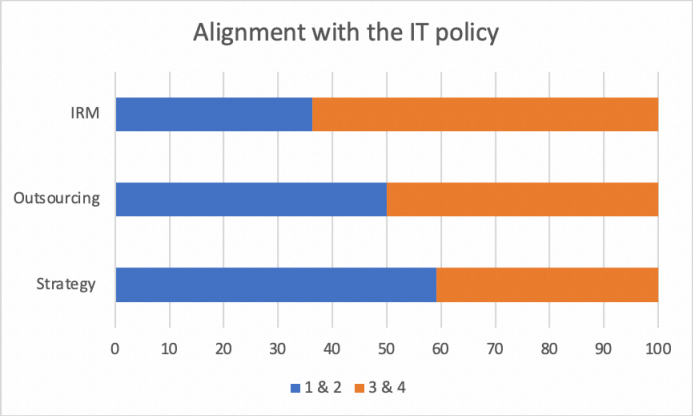

Figure 16 The alignment in percentage between IT and strategy, outsourcing and IRM. 1 is not aligned, 2 is not sufficiently aligned, 3 is aligned, 4 is fully aligned. 1&2 and 3&4 are grouped for visibility of the graph.

Gap 9: Insufficient alignment between the governance domains of pension funds.

In order to effectively implement information and cybersecurity, the governance aspects must be aligned. Information and cybersecurity affect all the different governance domains of the pension fund. Therefore, the required state is that the governance domains are aligned with a minimum of 3, preferably higher. The survey shows that a on average, half of the pension funds have poor alignment between the different governance aspects. This shows that a gap can be identified regarding the alignment between the different governance aspects.

Improvement 9: Improving the alignment between the governance domains

In order to effectively implement information and cybersecurity, pension funds must align their governance aspects. A prerequisite for this improvement is that a pension fund must have an IT policy. Pension fund must actively improve the alignment between their IT policy and the governance domains, including the strategy of their fund. The IT policy must be interwoven into the IRM, Outsourcing and Strategy policy. The alignment must be periodically updated and evaluated to ensure the alignment between the governance domains.

Validation

The topic of alignment between governance domains is validated among pension fund board members. The majority of the pension funds stated that they have some form of alignment, but this could be further improved. The reason that this has not been done is the lack of time and priority of the pension fund board.

4.5.3 IT risk appetite

Current state 10: Not all pension funds have formulated an IT risk appetite

The results of the survey provided insight into pension funds that have formulated a risk appetite and showed that on average, 74% of the responding pension funds had formulated an IT risk appetite. As a follow-up question, they were asked for which different IT domains an IT risk appetite has been drafted, see figure 17. 82% of the responding funds has formulated an IT risk appetite for the IT domain pension administration, 73% for the IT domain board environment and 68% for the IT domain asset management. This shows that not all pension funds have formulated an IT risk appetite.

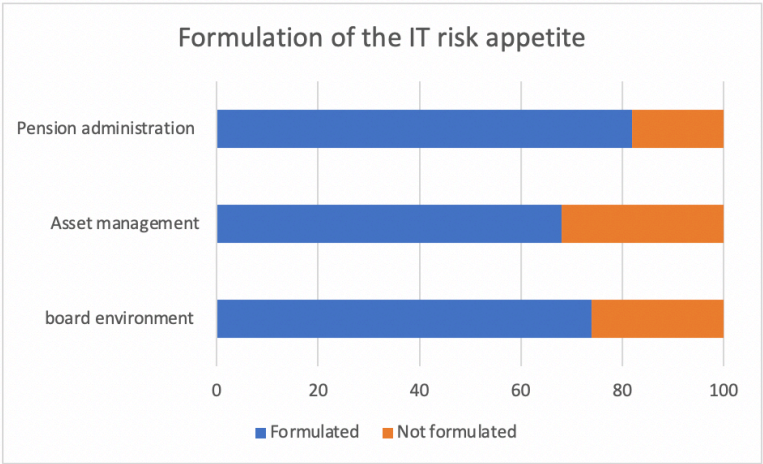

Figure 17: The formulation of the IT risk appetite within the different IT domains

Gap 10: Not all pension funds have formulated an IT risk appetite.

Laws and regulation require pension funds to have adequate procedures and measures implemented to manage IT risks. It is essential to have an IT risk appetite in order to manage IT risks.

The survey showed that not all responding pension funds have a risk appetite formulated where the aspects of availability, integrity and confidentiality of data (processing) have been taken into account. A gap can be identified that not all pension funds have formulated an IT risk appetite for the different IT domains.

Improvement 10: Formulation of a qualitative IT risk appetite.

An IT risk appetite is one of the prerequisites for managing IT risks. Pension fund must have an IT risk appetite formulated. This improvement focusses on the existence and the quality of the IT risk appetite. If pension funds don't have a risk appetite, they must formulate one. Suppose the pension fund already has an IT risk appetite. In that case, they must review it to check if it is in line with their risk strategy and if the risk appetite has incorporated the aspects of availability, integrity and confidentiality of data (processing). The IT risk appetite must be periodically reviewed and adjusted if necessary.

Validation

The topic of IT risk appetite is validated among pension fund board members. All pension funds have formulated an IT risk appetite, only the quality was different. Some pension fund have defined generic IT risks, only partly based on their IT risk assessment and their IT landscape. Others had formulated it based on their own IT risk assessment and categorized the risks based on the concepts of confidentiality, integrity and availability. It shows that the IT-risk appetite is defined within the pension fund, but that the quality differs.

4.5.4 Summary: DNB guidance documents
General state: Pension funds have a good fundamental basis for managing information and cybersecurity, but improvements can be made.
All responding pension funds have incorporated the governance aspects of outsourcing and IRM; only the adoption of an IT policy can be an improvement. Half of the responding pension funds have their governance domains aligned, which can be further improved. In addition, most of the pension funds have formulated an IT risk appetite. Although the majority has implemented the IT risk appetite, the quality can be further improved by aligning it with the strategy of the fund and if the aspects of availability, integrity and confidentiality of data (processing) are incorporated.

Chapter 5: The ICS improvement model

The ICS improvement model stands for Information Cybersecurity improvement model. In the following chapter, the ICS improvement model will be elaborated upon. The model is based upon the identified improvements as described in chapter 4. Practical implementation will be given to these improvements by incorporating them into a Plan-Do-Check-Act (PDCA model). For each of the phases of the PDCA model, the rationale and the goals of the phase will be elaborated upon. A detailed description of the activities and /or deliverables for each of the phases will be stated in appendix E.

5.1 Devised improvements

The following improvements are devised as a result of the gap analysis performed in chapter 6. The improvements are linked to the activities and/or deliverables stated in the ICS improvement model.

Table 10: Table of devised improvements in relation to topics within the ICS improvement model

#	Description improvement	Topic within the ICS improvement model
1	Creating awareness of information and cybersecurity within the pension fund board to increase adoption rate of the DNB Good Practice framework.	Prerequisite 2 Global aim of the ICS improvement model
2	Improving the usage of scenario-based testing and training within the fund and in the outsourcing chain.	B1. Awareness and training plan B2. Awareness and training exercises B3. Monitoring awareness and training B4. Awareness and training improvement plan
3	Improving the threat intelligence and impact analysis for pension funds.	Prerequisite 3 A3. Continuous threat analysis
4	Increasing the percentage of pension funds that have a comprehensive overview of their IT landscape.	Prerequisite 4 A1. Identification of the IT landscape
5	Improving the correct usage of accountability reports with the correct scope and depth.	Prerequisite 4
6	Adoption of IT requirements in the suitability plans of the pension fund.	Prerequisite 1
7	Increasing the level of IT knowledge among pension fund board members regarding IT and the outsourced IT domains.	B1. Awareness and training plan B2. Awareness and training exercises B3. Monitoring awareness and training B4. Awareness and training improvement plan
8	Drafting of the IT policy.	Prerequisite 5
9	Improving of the alignment between the governance aspects	Prerequisite 7
10	Formulation of a qualitative IT risk appetite.	Prerequisite 6

5.2 Prerequisites for the ICS improvement model

The following prerequisites must be in place for the effective use of the ICS improvement model.

1. The pension funds must have drafted a suitability policy that includes IT requirements and these requirements have been met, or development plans are in place that will achieve this.
2. The DNB Good Practice framework is implemented within the organisation.
3. For the IT domains pension administration and asset management, sectoral threat intelligence must be established for the pension fund. The IT domain within the board environment must have a proactive stance regarding informing the pension fund board regarding general IT threats.
4. Contractual agreements are made between the pension funds and the managed service provider regarding the outsourced services, processes and accountability reports. This is based on the principle of proportionality.
5. Pension funds must have a policy framework addressing IT, information and cybersecurity.
6. The pension fund has a qualitative IT risk appetite formulated where the aspects of confidentiality, integrity and availability are safeguarded and are in line with the risk strategy of the fund.
7. Pension funds must have aligned their governance domains and periodically review and update this.

5.3 ICS improvement model

The ICS improvement model aims to increase the cyber resilience of the pension funds.
This can be achieved by embedding information and cybersecurity within the DNA of the fund. By making board members aware of information and cybersecurity, the subject will come to life within the fund and will receive the attention it requires. The aim is to ensure sufficient awareness and knowledge within the fund to intrinsically motivated pension fund board members to tackle the topic of information ad cybersecurity. This will results in a pension fund that is cyber resilient. The ICS improvement model describes the following aspects for pension funds:

- what plans pension funds must-have for dealing with information and cybersecurity (plan)
- what measures must be implemented for dealing with information and cybersecurity risks (do)
- what check must be made to monitor if the measures are effective (check)
- what actions must be taken if this is not the case (act)

These four phases contribute to the aim of the improvement model.

The ICS improvement model is based on the plan-do-check-act cycle (PDCA cycle), also known as the Deming cycle for continuous improvement. The PDCA cycle is chosen because the DNB Good Practice framework and the NIST framework also have a form of the PDCA cycle implemented. This makes it possible to use the ICS improvement model supplementary to the existing frameworks.

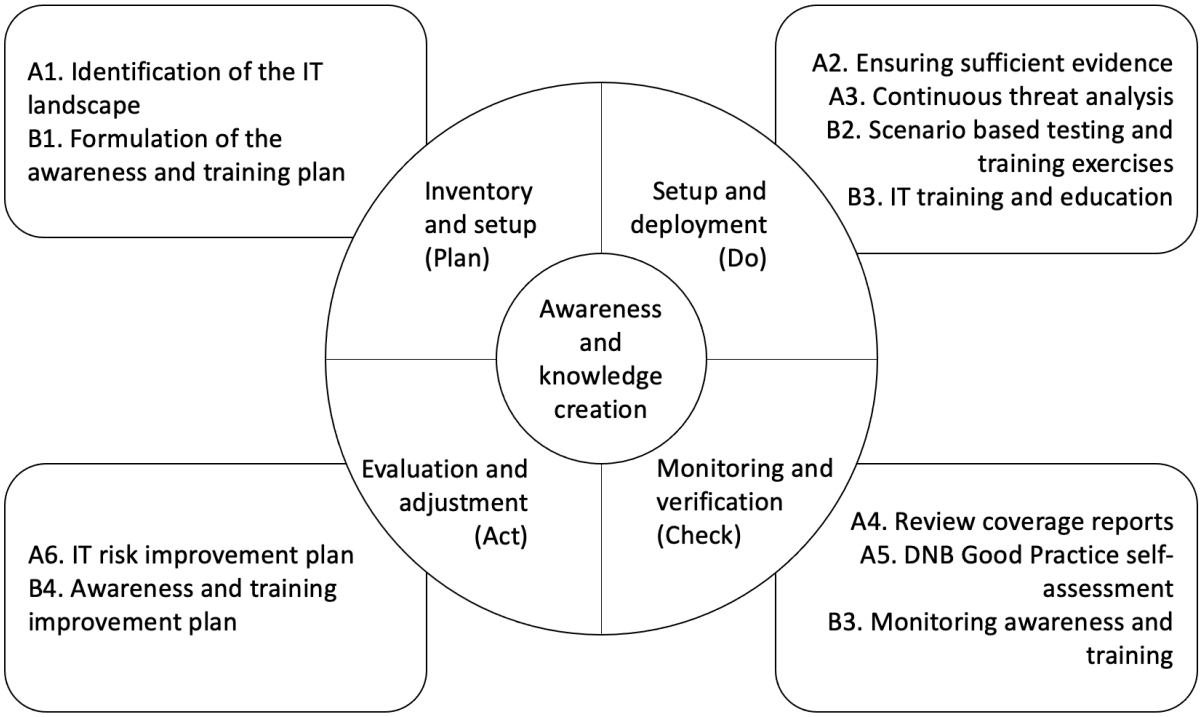

Figure 18: The ICS improvement model

The addressed improvements of the ICS improvement model are categorized into two themes:
A. The DNB Good Practice related topics
B. Awareness, knowledge and countervailing power related topics

5.3.1 Inventory and setup (plan)

The first phase of the ICS improvement model is inventory and setup (plan) phase. The global aim of this phase is the identification of the problems, opportunities and objectives and record this into a plan. If a pension fund has already gone through the cycle once, the results of the act phase can be used input for the plan phase.

A1. Identification of the IT landscape. The first step of the IT risk assessment is the identification of the landscape for all the IT domains of the fund.

B1. An awareness and training plan is drafted for the fulfilment of the drafted IT requirements of the suitability policy and specific information and cybersecurity training exercises where the DNB Good Practice fell short.

5.3.2 Setup and deployment (Do)

The second phase of the ICS improvement model is the setup and deployment (do) phase. The global aim of this phase is the execution of the plans defined in the plan phase.

A2. Pension funds ensure that sufficient evidence will be obtained in order to monitor the implemented information and cybersecurity controls.

A3. Continuous threat analysis is performed to identify new information or cybersecurity-related updates for the different IT domains

B2. Scenario-based testing and training exercises are performed with managed service provides.

B3. Pension fund board members follow training and education regarding information and cybersecurity.

5.3.3 Monitoring and verification (check)

The third phase of the ICS improvement model is the monitoring and verification (check) phase. The global aim of this phase is monitoring and verifying that the different drafted objectives are achieved.

A4. The accountability reports are received, as agreed upon in the contractual agreements with the managed service providers. These accountability reports are reviewed to validate the effectiveness of the implementation of the controls.

A5. Based on the results of the validation of the accountability reports, the DNB Good Practice self-assessment is performed.

B4. The (individual) results of the awareness and training exercises are monitored and the awareness and knowledge development plans of the board members are monitored and verified to assure that drafted requirements are met.

5.3.4 Evaluation and adjustment (act)

The last phase of the ICS improvement model is the evaluation and adjustment (act) phase. The global aim of this phase is to evaluate the results of the check phase and make adjustments accordingly. Pension fund must continuously improve their information and cybersecurity to not fall behind and become a target for cybercriminals.

A.6 Based on the results of the DNB Good Practice self-assessment and the accountability reports, possible gaps can be identified, and actions are taken to bridge these gaps. Action that cannot be resolved immediately is recorded in the IT risk improvement plan for the next improvement cycle.

B5. Based on the results of the monitoring of the awareness and training progress, gaps can be identified, and actions are taken to bridge these gaps. Actions that cannot be resolved immediately are recorded in the awareness and training improvement plan for the next improvement cycle.

5.4 Validation of the ICS improvement model

The ICS improvement model has been validated by a total of three pension fund board members. Two of the board members fulfilled a board member functions at other pension funds and provided also insights from that perspective.

The following questions were asked for the validation of the ICS improvement model:

1. On a scale from 1 to 10, to what extend could this model, in combination with the defined preconditions, can help your pension fund to manage information and cybersecurity more effectively?
   Response:

Board member 1	Board member 2	Board member 3
7	8	8

2. On a scale from 1 to 10, to what extend could this improvement model be applied to the current risk framework of the pension fund?
   Response:

Board member 1	Board member 2	Board member 3
8	8	8

3. On a scale from 1 to 10, to what extend could this model improve the awareness of information and cybersecurity among board members of the pension fund?
   Response:

Board member 1	Board member 2	Board member 3
8	8	8

4. Are there certain aspects missing or could certain aspects be improved of the improvement model?
   a. A certain trigger for information and cybersecurity where pension fund board members can monitor their progress regarding information and cybersecurity. For example, pension fund board members are always interested in the coverage ratio of the fund. A similar trigger can be used for information and cybersecurity.
   b. A possible light version of the improvement model designed for smaller pension funds.

The gaps and improvements on which the ICS improvement model is based upon, are presented to a director of the DNB, who helped with the creation of the DNB Good Practice framework. The identified gaps were recognized by the DNB and the improvements were said to be good ways to overcome the identified gaps.

Chapter 6: Conclusion

6.1 Answers to the research questions

Main research question

How can pension funds integrate information and cybersecurity in their critical business processes in order to ensure reliable and controlled business operations?

Sub-question 1: What is the required state of information and cybersecurity for pension funds and their managed service providers?

Three aspects have been identified that contribute to the required state of information and cybersecurity for pension funds and their managed service providers. Each of the following aspects contributes to the overall current state:

- The DNB Good Practice framework

In order to effectively manage information and cybersecurity, pension funds must implement the DNB Good Practice framework. The DNB Good Practice framework provides a solid base for pension funds however falls short on certain aspects. The ICS improvement model addresses these aspects and helps pension funds to improve the state of information and cybersecurity.

- Knowledge, experience and countervailing power

Knowledge, experience and countervailing power regarding IT must be safeguarded within the pension fund board. This can be achieved by periodic educational session, trainings and exercises that increase the level of knowledge and awareness regarding IT.

- Governance domains of pension funds

The governance domains of the pension fund: IT, IRM and outsourcing must be all implemented and aligned with each other, forming an effective base for managing IT. The governance domains must contribute to the alignment between the business demands of the pension fund and the IT supply of the managed service provider.

Sub-question 2: What is the current state of information and cybersecurity of pension funds in the Netherlands?

The current state of information and cybersecurity of pension funds in the Netherlands is identified by surveying pension funds. The current state is described per identified aspects that contribute to the overall state of information and cybersecurity.

- The DNB Good Practice framework

The DNB Good Practice framework adoption rate is low at responding pension funds. In addition, the pension funds using the DNB Good Practice framework fall short on the control aspects of awareness and education, incident response and recovery.

- Knowledge, experience and countervailing power

Board members of Dutch pension funds have insufficient knowledge and experience safeguarded within their pension funds regarding IT, information and cybersecurity. Pension funds are not able to sufficiently safeguard their countervailing power over their outsourced activities with the current level of knowledge and experience regarding IT, information and cybersecurity.

- Governance domains of pension funds

Almost all pension funds have given substance to the various governance domains of IT, IRM and outsourcing. However, the alignment between the governance domains can be improved.

Sub-question 3: Is there a gap between the required state and the current state? If so, what are the steps that need to be taken to reach an adequate and proportional level of cyber resilience?

During the gap analysis, the current state of pension funds is compared to the required state for the identification of gaps regarding information and cybersecurity. For each of the identified gaps, improvements are devised to improve the cyber resilience of the pension funds. The following 10 gaps are identified during the gap analysis:

1. The adoption rate of the DNB Good Practice framework within pension funds is low
2. Scenario-based testing and training in the pension funds and cooperation with the managed service providers is insufficient
3. The current pension funds ISAC is not sufficient enough for pension funds
4. A low percentage of pension funds have an overview of their IT landscape
5. A low percentage of pension funds obtain accountability reports regarding the topics of information and cybersecurity with the correct scope and depth
6. A low percentage of pension funds has IT requirements for pension fund board members incorporated in their suitability plans
7. There is insufficient IT experience and knowledge safeguarded within the pension fund board
8. Not all pension funds have an IT policy
9. There is insufficient alignment between the governance domains of pension funds
10. Not all pension funds have formulated an IT risk appetite

Sub-question 4: What instruments can be used to help pension funds reach an adequate and proportional level of cyber resilience?

The devised improvements are anchored within the ICS improvement model, see figure 18, that provides the practical substance for pension funds to increase the cyber resilience of the fund. The ICS improvement model can be used as a supplemental model on top of the DNB Good Practice framework to further improve the information and cybersecurity stance of the pension fund. The ICS improvement model emphasizes on the aspects the DNB Good Practice fell short.

Main research question: How can pension funds integrate information and cybersecurity in their critical business processes in order to ensure sound and controlled business operations?

Pension funds can integrate information and cybersecurity within their critical business processes to ensure sound and controlled business operations by implementing the following three aspects:

The first aspect is that pension funds must correctly implement the DNB Good Practice framework combined with the ICS improvement model to have controls in place that ensure sound and controlled business operations.

The second aspect is that the pension fund board must be more aware of the importance of information and cybersecurity. Pension funds must have knowledge and experience safeguarded within the board to have enough countervailing power to manage their outsourcing activities. The pension fund board must be a fully-fledged discussion partner for IT, information and cybersecurity-related topics. It cannot be expected that pension fund board members are experts on the topic, however, enough countervailing power must be safeguarded to manage their IT processes. Finally, the pension fund board members must intrinsically want to improve the fund's cyber resilience continuously.

The third aspect is that the IT governance domains of the pension fund must be aligned. The domains IT, outsourcing and IRM, must be aligned, and the IT policy must be interwoven into the outsourcing domain and in the IRM domain. The three IT governance domains must contribute to the alignment between the pension fund and the managed service provider.

By integrating these three aspects into the pension fund’s critical business processes, the sound and controlled business operation can be sufficiently safeguarded.

6.2 Contributions

The contributions of this thesis are the following:

1. The ICS improvement model
2. Identification of the current state and the required state of pension funds
3. Identification of the gaps
4. Recommendations to the supervisory authority

6.3 Limitations

One of the limitations of the survey was the amount of pension funds that responded to the survey. 25 Pensions funds responded and provided data for this research, covering around 14% of the pension sector. In addition to this, the responding pension funds were selected through the network of KoutersVanderMeer which can cause a selection bias.
Another limitation was that knowledge and expertise regarding the topics of the survey among pension fund board members. After the survey, contact was sought with pension funds that completed the survey. The responding pension funds found the questions sometimes hard to answer because they lacked the knowledge. This lack of knowledge regarding information and cybersecurity was also a result of the survey and could case the representativeness heuristic bias. By not completely understanding the question, pension fund board members could have given themselves the benefit of the doubt regarding information and cybersecurity-related topics. The last limitation was the limited validation of the results. Three pension funds board members were interviewed for the validation of the gaps, improvements and the ICS improvement model.

6.4 Final observations

The results of this thesis show that the responding pension funds are not entirely cybercrime resilient. One of the aspects that contributed to this was the insufficient IT knowledge and experience of pension fund board members. This topic was discussed with more than ten pension fund board members. The general reaction on this topic was that they agreed that some form of IT knowledge must be safeguarded within the fund. Although IT is a small part, it is often overlooked. This was partly due to outsourcing all the IT processes and the high level of trust between the pension funds and their managed IT service providers. This was common among responding pension funds, only a couple of pension funds were intrinsically motivated for the management of information and cybersecurity.

Pension funds are ultimately responsible for their information and cybersecurity. From the perspective of a pension fund board member, it could be argued that the increasing digitalization of pension funds in the Netherlands transforms pension funds into companies that manage information rather than traditional pension funds that collect pension premiums and disperse pension payments. Therefore, it is important that pension funds must become aware and knowledgeable of the IT side of the pension funds instead of being primarily focused on the financial side. Where exactly the responsibilities of information and cybersecurity should lie must be further investigated. Nevertheless, it is necessary that the level of knowledge and experience regarding IT, information and cybersecurity must be further increased.

6.5 Further research

This research provides various directions for future studies. The first direction for future studies arose after interviews with various experts on the subject. The responsibility for managing information and cybersecurity lies currently at the pension fund board but is primarily managed by pension fund service providers. Pension funds do not have the in-depth knowledge and experience to manage this and therefore a future study can be performed to research the shift of responsibilities of information and cybersecurity. The DNB is currently performing a pilot within the pension administration domain where the main focus is placed on the pension administration instead of pension funds.

The second direction for future research is regarding the determination of the level of knowledge and experience of pension fund board members regarding information and cybersecurity. During this research, mainly global questions were asked about knowledge and experience, but the in-depth knowledge of pension fund board members was out of the scope of this research.

The third direction for future research is to address the possible biases identified in the limitations. Only around 15% of the pension sector is researched and primarily within the network of KoutersVanderMeer. Future research could examine more pension funds to obtain a complete overview of the pension sector.

The last direction for future research is the implementation and the fine-tuning of the ICS improvement model. This research focusses on developing a model to help improve the cyber resilience of pension funds but implementing and testing the model was beyond the scope.

Bibliography

1FTL-NL. (2019). *1 Financial Threat Landscape for the Netherlands.* 1FTL.

Almuhammadi, S. &. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT) 7*, 51-62.

Analistennetwerk Nationale Veiligheid. (2016). *Nationaal Veiligheidsprofiel 2016.* Bilthoven : Rijksinstituut voor Volksgezondheid en Milieu.

Arora, V. (2010). Comparing different information security standards: COBIT v s. ISO 27001. *Qatar: Carnegia Mellon University.*

Baveco, M. (2015, december 17). *Effect creëren in de boardroom The next level: effect bereiken.* Retrieved from deitauditor.nl: https://www.deitauditor.nl/risicomanagement/the-next-level-effect-bereiken/

Belcourt, M. (2006). Outsourcing—The benefits and the risks. *Human resource management review*, 269-279.

Björck, F. H. (2015). Cyber resilience–fundamentals for a definition. *New contributions in information systems and technologies*, 311-316.

Bodeau, D. G. (2011). *Cyber resiliency engineering framework.* MITRE Corporation.

Cui, Q. J. (2017, april). Tracking phishing attacks over time. *In Proceedings of the 26th International Conference on World Wide Web* , pp. 667-676.

De nederlandsche bank . (2020). *Open boek toezicht* . Retrieved from Governance: uitbesteding : https://www.toezicht.dnb.nl/2/5/50-230431.jsp

De Nederlandsche Bank. (2017). *Financiele Kern Infrastructuur.* Amsterdam : De Nederlandsche Bank.

De Nederlandsche Bank. (2018). *Information security Monitor 2018.* Amsterdam : De Nederlandsche Bank.

De Nederlandsche Bank. (2018, January 18). *Seminar informatiebeveiliging en cybersecurity.* Retrieved from www.dnb.nl: https://www.dnb.nl/binaries/Presentaties%20DNB%20seminar%20informatiebeveiliging_tcm46-373188.pdf

De Nederlandsche Bank. (2019). *Gegevens individuele pensioenfondsen (Jaar).* Retrieved from statistiek.dnb.nl: https://statistiek.dnb.nl/downloads/index.aspx#/details/gegevens-individuele-pensioenfondsen-jaar/dataset/78c1c804-0b65-4bbc-a5cc-df9cd75c9ded

De Nederlandsche Bank N.V. (2016). *Technological innovation and the Dutch Financial Sector* . Amsterdam: De Nederlandsche Bank.

De Nederlandsche Bank N.V. en de Stichting Autoriteit Financiële Markten. (2020, mei 25). *Beleidsregel geschiktheid 2012.* Retrieved from DNB: https://www.toezicht.dnb.nl/binaries/50-238118.pdf

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *information security management.*

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.

DNB. (2012). *FOCUS! De vernieuwde toezichtaanpak van de DNB.* Amsterdam.

DNB. (2018). *IB monitor 2018.* DNB.

DNB. (2018, februari 23). *Sector terugkoppeling resultaten Informatiebeveiliging / Cyber onderzoek 2017 bij verzekeraars en pensioenfondsen.* Retrieved from dnb.nl: https://www.dnb.nl/binaries/1%20Sector%20terugkoppeling%20resultaten%20Informatiebeveiliging%20%20-%20Cyber%20onderzoek%202017%20bij%20verzekeraars%20en%20pensioenfondsen_tcm46-373187.pdf

DNB. (2018). *Terugkoppeling onderzoek 'inventarisatie uitbesteding'.* Amsterdam: DNB.
DNB. (2020). *Jaarlijkese informatiebeveiligingsmonitor.* De Nederlandsche Bank.
DNB. (2020, Januari 24). Statistisch Nieuwsbericht: Financiële positie pensioenfondsen verbeterd. *DNB*.
DNB. (2020). *Uitbesteding door pensioenfondsen*. Retrieved from https://www.toezicht.dnb.nl/: https://www.toezicht.dnb.nl/2/6/50-236728.jsp
Earl, M. J. (1996). The risks of outsourcing IT. *Sloan management review 37* , 26-32.
Frissen, T. &. (2019). *Nulmeting digitale transformatie in boardrooms in Nederland.* Den Haag : Nationaal Register en Nederland ICT .
Garousi, V. F. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering . *Information and Software Technology 106*, 101-121.
Healthcare Dive. (2020, 08 12). *healthcaredive.com*. Retrieved from NHS targeted with over 40,000 phishing emails during Covid-19 outbreak: https://www.healthcaredive.com/press-release/20200812-nhs-targeted-with-over-40000-phishing-emails-during-covid-19-outbreak/
Information Security Forum. (2011). *Cyber Security Strategies: Achieving cyber resilience.* . Retrieved from Security Forum: https://www.securityforum.org/research/cyber-security-strategies-achieving-cyber-resilience/
ISACA. (2009). The Risk IT practitioner Guide. In ISACA, *The Risk IT practitioner Guide.* Rolling Mead.
ISACA. (2019). *COBIT 2019 framework: introduction & Methodology.* Schaumburg : ISACA.
ISO/IEC 27002. (2013). *code of practice for information security management.*
ISO/IEC 27002. (2013). *ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls.*
ITU. (2009). *SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY.* Geneva . Retrieved from ITU: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
Jordan, E. &. (2005). Beating IT risks. John Wiley & Sons.
Kakabadse, A. &. (2005). Outsourcing: current and future trends. . *Thunderbird international business review, 47(2)*, 183-204.
Klijnsma, J. (2014). *Brief regering; Risico's van uitbesteding door pensioenfondsen - Toekomst pensioenstelsel.* Den Haag : Ministerie van sociale zaken en werkgelegenheid.
Maes, R. (1999). A generic framework for information management. . *Department of Accountancy & Information Management.*
Martin, P. Y. (1986). Grounded theory and organizational research. *The journal of applied behavioral science, 22*, 141-157.
Merali, Y. &. (2006). Using Complexity Science to effect a paradigm shift in Information Systems for the 21st century. . *Journal of Information Technology, 21(4)*, 211-215.
Mooy, C. d. (2020). *Over verjonging, diversiteit en vertrouwen in de pensioensector*. Retrieved from Whyz: https://www.whyz.nl/blogs/als-je-doet-wat-je-deed-krijg-je-wat-je-kreeg/#
National Cyber Security Centre. (2018). *Nationale cyber security agenda* . Den Haag: Minsterie van Justitie en Veiligheid.
NCTV. (2020). *overzicht vitale processen*. Retrieved from NCTV.nl: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen
NIST. (2018). *Framework for Improving Critical Infrastructure.* National Institute of Standards and Technology. National Institute of Standards and Technology.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* National Institute of Standards and Technology.
NOREA. (2015). *Analyse Cyber Security Standaarden en Frameworks* . NOREA.
NOS. (2020, 05 02). *NOS*. Retrieved from NOS.nl: https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaald.html
Ottis, R. &. (2010). Cyberspace: Definition and implications. In International Conference on Cyber Warfare and Security. *Academic Conferences International Limited.*, 267.
Pensioen Federatie. (2014). *Handreiking geschikt pensioenfondsbestuur.* Den Haag.
S. Ghafur, S. K. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj digital medicine 2*.
Saltzer, J. H. (1975). the protection of information in computer systems. *Proceedings of the IEEE 63(9)*, 1278-1308,.
Simchi-Levi, D. K.-L. (2004). *Managing the supply chain.*
Staatssecretaris van sociale zaken en werkgelegenheid. (2014, januari 17). *Brief regering; Risico's van uitbesteding door pensioenfondsen - Toekomst pensioenstelsel.* Retrieved from https://www.parlementairemonitor.nl: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vjgnfrok50y7
Stabel, D.L. (2020, februari). IT in control aan de bestuurstafel. *Pensioen Managinze*, p. 15.
Talsma, I. (2018, april). Uitbesteding: groeien. *Pensioen, bestuur & management* .
Threa, F. (n.d.).
Von Solms, R. &. (2013). From information security to cyber security. *computers & security, 38,*, 97-102.
Vossen, A. (2015, juli 1). *'Beheersing IT risico's moet hoger op de bestuursagenda'*. Retrieved from DNB: https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-pensioenen/nieuwsbrief-pensioenen-juli-2015/dnb323390.jsp
Westerman, G. F. (2006). *It risk management: from It necessity to strategic business value.*
Whitman, M. E. (2011). Principles of information security. Cengage Learning.

Appendix

A. Explorative interviews

Explorative interview questions:

1. Can you explain how the pension fund's governance model is set up and how decisions are made?
2. How is the 1st, 2nd, 3rd line composed with key function holders and fillers?
3. How does the pension fund gain insight into its IT risks?
4. How are IT risks controlled and managed by the board?
5. How are IT risks taken into account in the outsourcing process?
6. How is expertise in the field of IT and cyber risks ensured within the board?
7. Who is responsible for cybersecurity on the board?
8. Does the board pay attention to responding to possible cyber-attacks based on scenarios?
9. How is the board of the pension fund kept informed of the developments in the cyber field by the managed service providers?

Summary explorative interview

Pension funds board members interviewed: 3. Results are summarized and presented in bullets

IT within the board of pension funds

- There are generally no pension fund board members with an IT-background
- Pension funds are more focussed on financial risks than IT related risks.
- Pension funds board meeting have around 80 agenda items, IT only has a small role, information and cybersecurity even smaller

Knowledge and awareness regarding information and cybersecurity

- Knowledge and awareness regarding information and cybersecurity is low.
- Information and cybersecurity are handled on an incident driven basis.
- Education and training regarding IT only 1 or 2 times a year.
- Board members are less likely to admit they miss out knowledge and experience regarding IT.

IT risks

- ISAE reports provides limited insights in the IT risks
- IT, information and cybersecurity plays a small role in monthly meetings
- Based in incidents, information is requested of managed service providers regarding information and cybersecurity.

Outsourcing and IT risks

- Reports regarding the outsourcing relationship are obtained on a yearly basis.
- Based on the obtained ISAE reports, pension funds can use external audits to extra validate the controls. I
- Focus is more on financial risks than IT risks
- SLA are used to manage the outsourcing agreements; IT is often not included.
- Lot of trust on the outsourcing relationship for managing IT risks

Information and cybersecurity

- No scenario-based testing
- No crisis plans available for cyber incidents
- No periodic testing
  less than 5 times a year contact with the managed service provider regarding information and cybersecurity.

B. Survey Design

The survey to map the current state of cybersecurity in the pension sector. The survey contained 37 questions and was sent to 54 different pension funds. Of the 54 pension funds, 25 pension funds have filled in the survey.

The survey was divided into four section, each mapping a different aspect related to managing cybersecurity. The four sections are:

- General questions regarding the fund
- Guidance documents
- Suitability plans
- Managing information and cybersecurity

General question regarding the fund.

The first six questions were about gaining information regarding the fund and the person filling in the survey. These questions answered the following:

- Function of the person filling in the survey
- The type of pension fund they are filling it in for
- The size of the fund
- If the board of the fund is supported by a board office.
- The governance model of the board
- The amount of board members
- And if they participated in investigations of the DNB

IT risk management question

The IT-risk management questions are divided into the three IT domains:

- Board environment
- Pension administration
- Asset management

The questions asked in the survey related to the three different IT-domains. The questions answered the following:

- Outsourced activities
- Types of assurance reports
- Overview of the IT chain
- Policy documents regarding outsourcing, risk management and IT.

Suitability plans

The questions regarded the suitability plans and the expertise and knowledge of pension fund board members answered the following:

- The expertise and knowledge of board members regarding IT.
- The requirements for pension fund board members regarding expertise and knowledge.

Managing information and cybersecurity.

The last section of the survey answered question regarding information and cybersecurity. The questions of the survey answered the topics of:

- Scenario based testing
- Testing in the outsourcing chain
- Types of cybersecurity tests
- Expertise regarding cybersecurity related topics

C. Survey Results

Default Report
Survey cybersecurity in de pensioensector
November 28th 2020, 3:55 am MST

Q1.3 - Onderdeel 1: Vragen over het fonds en de wijze waarop IT-risicobeheersing is vormgegeven. 1. Wat is uw functie binnen het fonds

#	Answer	%	Count
1	Manager Bestuursbureau: Directeur / Manager Bestuursbureau / Pensioenbureau.	24.00%	6
2	Overig	48.00%	12
3	Bestuurslid met IT-verantwoordelijkheid (1e lijn).	28.00%	7
	Total	100%	25

Q1.4 - 2. Namens wat voor soort pensioenfonds vult u deze survey in?

#	Answer	%	Count
1	Ondernemingspensioenfonds (OPF)	60.00%	15
2	Bedrijfstakpensioenfonds (BPF)	36.00%	9
3	Beroepspensioenfonds (BRP)	4.00%	1
4	Algemeen Pensioenfonds (APF)	0.00%	0
5	Premie Pensioeninstelling (PPI)	0.00%	0
6	Overig, namelijk	0.00%	0
	Total	100%	25

Q1.5 - 3. De Nederlandsche Bank gebruikt de Toezicht klasses om pensioenfondsen te classificeren op de grootte van het fonds. Tot welke T-klasse behoort uw pensioenfonds? Indien u niet weet in welke T-klasse uw fonds is ingedeeld, hanteert u dan de volgende criteria:

#	Answer	%	Count
1	T1 (kleine, liquiderende of volledig herverzekerde fondsen, tot 1 miljard beheerd vermogen)	28.00%	7
2	T2 (middelgrote fondsen, tussen 1 miljard en 5 miljard beheerd vermogen)	40.00%	10
3	T3 (grote fondsen, meer dan 5 miljard beheerd vermogen)	28.00%	7
4	T4 (zeer grote pensioenfondsen, een van de vijf grootste pensioenfondsen van Nederland)	4.00%	1
	Total	100%	25

Q1.6 - 4. Wordt het fondsbestuur ondersteund door een bestuur bureau (zowel intern als extern betrokken)?

#	Answer	%	Count
1	Ja, onderdeel interne organisatie	52.00%	13
2	Ja, extern betrokken	28.00%	7
3	Nee	20.00%	5
	Total	100%	25

Q1.7 - 5. Hoe ziet het bestuursmodel van uw fonds eruit?

#	Answer	%	Count
1	Paritair bestuur (bestuurders zijn paritair, maximaal 2 externe bestuurders)	88.00%	22
2	Onafhankelijk bestuur (bestuurders zijn onafhankelijk)	0.00%	0
3	Paritair gemengd (uitvoerend bestuurders zijn paritair, max 2 externen)	4.00%	1
4	Onafhankelijk gemengd (uitvoerend bestuurders zijn onafhankelijk)	0.00%	0
5	Omgekeerd gemengd (uitvoerend bestuurders zijn onafhankelijk)	8.00%	2
	Total	100%	25

Q1.8 - 6. Hoeveel bestuurders telt de uitvoerend besturende laag van het pensioenfonds?

#	Answer	%	Count
2	1	0.00%	0
3	2	25.00 %	6
4	3	8.33%	2
5	meer dan 4, namelijk	62.50 %	15
6	4	4.17%	1
	Total	100%	24

Q1.9 - 7. Is uw fonds in de afgelopen drie jaar of wordt uw fonds in de nabije toekomst onderworpen aan, een of meerdere van de volgende, themagerichte onderzoeken van DNB?

	Field	Choice count	
1	Ja, Informatiebeveiliging & Cybersecurity	30.77%	4
2	Ja, Datakwaliteit	7.69%	1
3	Ja, Robuuste pensioenadministratie	23.08%	3
4	Ja, Uitbesteding	7.69%	1
5	Nee	23.08%	3
6	Ja, Overig namelijk	7.69%	1
			13

Q1.11 - De volgende vragen gaan over het IT-domein BestuursomgevingOnder het begrip IT-domein wordt verstaan: de onderverdeling van IT-applicaties, systemen en processen die bijdragen om de primaire bedrijfsprocessen van de Bestuursomgeving te kunnen realiseren.De bestuursomgeving ondersteunt het bestuur met activiteiten zoals, voorbereiden van beleidsdocumenten, communicatie met deelnemers en het toezicht houden op uitbestede activiteiten. 8. Heeft uw fonds haar IT-risicobereidheid geformuleerd voor het IT-domein Bestuursomgeving, waarbij de aspecten beschikbaarheid, integriteit en vertrouwelijkheid van gegevens(verwerking) in beschouwing zijn genomen?

#	Answer	%	Count
1	Ja	73.91%	17
2	Nee	26.09%	6
	Total	100%	23

Q1.12 - 9. Welke IT-middelen heeft uw fonds uitbesteed of betrokken van derden om de processen binnen het IT-domein Bestuursomgeving te ondersteunen? (aanvinken welke IT-middelen uitbesteed zijn)

#	9. Welke IT-middelen heeft uw fonds uitbesteed of betrokken van derden om de processen binnen het IT-domein Bestuursomgeving te ondersteunen? (aanvinken welke IT-middelen uitbesteed zijn) - Selected Choice	Percentage
1	Bestuursportaal	17.31%
2	E-mailvoorziening t.b.v. interne en externe communicatie	16.35%
3	Bestandsopslag (file server, cloud storage)	18.27%
4	Werkplekken (laptops, tablets en smartphones)	14.42%
5	Vergaderen (beeldbellen en telefonie)	15.38%
6	Wettelijk verplichte rapportages DNB	16.35%
7	Overig, namelijk:	1.92%
8	Geen	0.00%
	Total	104

Q1.13 - 10. Welke soorten verantwoordingsrapportages over IT-beheersing binnen het IT-domein Bestuursomgeving ontvangt u van uw uitbestedingspartner(s)?

#	Answer	%	Count
1	SLR-rapportage	13.92%	11
2	NFR-rapportage/ risico rapportage	15.19%	12
3	ISAE 3402	20.25%	16
4	ISAE 3000 (op basis van SOC2 standaard)	8.86%	7
5	ISO 27001	6.33%	5
6	Cyber volwassenheid rapportage	3.80%	3
7	Incidenten rapportage met IT- en cyberincidenten separaat gecategoriseerd	15.19%	12
8	Overig, namelijk	1.27%	1
9	Geen	2.53%	2
10	Resultaten self-assessment van DNB	12.66%	10
	Total	100%	79

Q1.14 - 11. Ontvangt u van uw uitbestedingspartner(s) binnen het IT-domein Bestuursomgeving jaarlijks een overzicht van de IT-keten die voor de dienstverlening aan het fonds is ingericht? Het overzicht van de IT-keten bevat minimaal: - Gebruikte applicaties per uitbesteed proces. - Kritieke of belangrijke onder uitbestedingen. - Locaties van dataopslag.

#	Answer	%	Count
1	Ja	50.00%	11
2	Nee	50.00%	11
	Total	100%	22

Q1.16 - De volgende vragen gaan over het IT-domein Vermogensbeheer Onder het begrip IT-domein wordt verstaan: de onderverdeling van IT-applicaties, systemen en processen die bijdragen om de primaire bedrijfsprocessen van vermogensbeheer te kunnen realiseren 12. Heeft uw fonds haar IT-risicobereidheid geformuleerd voor het IT-domein Vermogensbeheer, waarbij de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens(verwerking) in beschouwing zijn genomen?

#	Answer	%	Count
1	Ja	68.18%	15
2	Nee	31.82%	7
	Total	100%	22

Q1.17 - 13. Welke soorten verantwoordingsrapportages over IT-beheersing binnen het IT-domein vermogensbeheer ontvangt u van uw uitbestedingspartner(s)?

#	Answer	%	Count
1	SLR-rapportage	16.90%	12
2	NFR-rapportage / risico rapportage	18.31%	13
3	ISAE3402	30.99%	22
4	ISAE 3000 (o.b.v. SOC2 standaard)	7.04%	5
5	ISO 27001	4.23%	3
6	Cyber volwassenheid rapportage	1.41%	1
7	Incidenten rapportage met IT- en cyberincidenten separaat gecategoriseerd	14.08%	10
8	Resultaten self-assessment van DNB	7.04%	5
9	Overig, namelijk	0.00%	0
10	Geen	0.00%	0
	Total	100%	71

Q1.18 - 14. Welke primaire processen heeft uw fonds uitbesteed op het gebied van Vermogensbeheer? (aanvinken welke processen uitbesteed zijn)

#	Answer	Count
1	Portefeuillebeheer	20
2	Liquiditeit beheer	17
3	Compliance monitoring	18
4	Performance monitoring	20
5	Portefeuilleadministratie	21
6	Afwikkeling effecten en transacties	22
7	Bewaring effecten (custodian)	20
8	Overig, namelijk	1
9	Geen	0
	Total	/25

Q1.19 - 15. Ontvangt u van uw uitbestedingspartner(s) binnen het IT-domein Vermogensbeheer jaarlijks een overzicht van de IT-keten die voor de dienstverlening aan het fonds is ingericht? Het overzicht van de IT-keten bevat minimaal: - Gebruikte applicaties per uitbesteed proces. - Kritieke of belangrijke onder uitbestedingen. - Locaties van dataopslag.

#	Answer	%	Count
1	Ja	36.36%	8
2	Nee	63.64%	14
	Total	100%	22

Q1.21 - De volgende vragen gaan over het IT-domein PensioenbeheerOnder het begrip IT-domein wordt verstaan: de onderverdeling van IT-applicaties, systemen en processen die bijdragen om de primaire bedrijfsprocessen van pensioenbeheer te kunnen realiseren 16. Heeft uw fonds haar IT-risicobereidheid geformuleerd voor het IT-domein Pensioenbeheer,

waarbij de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens(verwerking) in beschouwing zijn genomen?

#	Answer	%	Count
1	Ja	81.82%	18
2	Nee	18.18%	4
	Total	100%	22

Q1.22 - 17. Welke soorten verantwoordingsrapportages over IT-beheersing binnen het IT-domein Pensioenbeheer ontvangt u van uw uitbestedingspartner(s)?

#	Answer	%	Count
1	SLR-rapportage	17.02%	16
2	NFR-rapportage/ risico rapportage	14.89%	14
3	ISAE3402	23.40%	22
4	ISAE 3000 (o.b.v. SOC2 standaard)	7.45%	7
5	ISO 27001	2.13%	2
6	Cyber volwassenheid rapportage	5.32%	5
7	Incidenten rapportage met IT- en cyberincidenten separaat gecategoriseerd	14.89%	14
8	Overig, namelijk	1.06%	1
9	geen	0.00%	0
10	Resultaten self-assessment van DNB	13.83%	13
	Total	100%	94

Q1.23 - 18. Welke primaire processen heeft uw fonds uitbesteed op het gebied van pensioenbeheer? (aanvinken welke processen uitbesteed zijn)

#	Answer	%	Count
1	Werkgeversadministratie	10.00%	11
2	Deelnemers en aansprakenadministratie	20.00%	22
3	Communicatie met de klant	18.18%	20
4	Communicatie en rapportage richting DNB	15.45%	17
5	Premie oplegging en incasso	14.55%	16
6	Excasso, pensioenbetalingen	19.09%	21
7	Overig, namelijk	2.73%	3
8	Geen	0.00%	0
	Total	100%	110

Q1.24 - 19. Ontvangt u van uw uitbestedingspartner(s) binnen het IT-domein Pensioenbeheer jaarlijks een overzicht van de IT-keten die voor de dienstverlening aan het fonds is ingericht? Het overzicht van de IT-keten bevat minimaal: - Gebruikte applicaties per uitbesteed proces. - Kritieke of belangrijke onder uitbestedingen. - Locaties van dataopslag.

#	Answer	%	Count
1	Ja	63.64%	14
2	Nee	36.36%	8
	Total	100%	22

Q1.26 - 20. Heeft uw fonds een geschiktheidsbeleid voor fondsbestuurders opgesteld? Een geschiktheid beleid is een document waarin de eisen op het gebied van kennis en ervaring zijn opgenomen waaraan de bestuurders van het fonds moeten voldoen

#	Answer	%	Count
1	Ja	95.45%	21
2	Nee	4.55%	1
	Total	100%	22

Q1.27 - 20.1. Is binnen het geschiktheidsbeleid expliciet aandacht voor benodigde vakinhoudelijke kennis en werkervaring op het gebied van IT?

#	Answer	%	Count
1	Ja	43%	9
2	Nee	57%	12
	Total	100%	21

Q1.28 - 21. Heeft u binnen de organisatie van het fonds een of meerdere personen met vakinhoudelijke kennis en relevante werkervaring met betrekking tot IT-aspecten?

#	Answer	%	Count
1	Ja	59 %	13
2	Nee	41%	9
	Total	100%	22

Q1.29 - 21.1 Bij welke IT domeinen is deze vakinhoudelijke kennis en relevante werkervaring met betrekking tot IT aspecten aanwezig?

#	Answer	%	Count
1	Binnen de bestuursomgeving	46%	11
2	Binnen het vermogensbeheer	17%	4
3	Binnen de pensioenadministratie	33%	8
4	Overig, namelijk	4%	1
	Total	100%	24

Q1.32 - Onderdeel 3: Vragen over activiteiten en maatregelen op het gebied van informatiebeveiliging en Cybersecurity. 22. Heeft uw fonds een beleidskader voor de beheersing van IT?

#	Answer	%	Count
1	Ja, beschreven in een apart specifiek document	64%	14
2	Nee	18%	4
3	Ja, opgenomen in ander beleidsdocument	18%	4
	Total	100%	22

Q1.33 - 23. Heeft uw fonds een beleidskader voor de beheersing van uitbesteding?

#	Answer	%	Count
1	Ja, beschreven in een apart specifiek document	91%	20
2	Nee	0 %	0
3	Ja, opgenomen in ander beleidsdocument	9%	2
	Total	100%	22

Q1.34 - 24. Heeft uw fonds een beleidskader voor risicomanagement

#	Answer	%	Count
1	ja, beschreven in een specifiek beleidsdocument	91%	20
2	ja, opgenomen in een ander beleidsdocument	9%	2
3	Nee	0%	0
	Total	100%	22

Q1.35 - 25. In hoeverre zit het beleidskader van IT verweven in het beleidskader van risicomanagement op een schaal van 1 tot 4?

#	Answer	%	Count
1	1, niet meegenomen	4.55%	1
2	2	31.82%	7
3	3	36.36%	8
5	4, volledig op elkaar afgestemd	27.27%	6
	Total	100%	22

Q1.36 - 26. In hoeverre zit het beleidskader van IT verweven in het beleidskader van uitbesteding op een schaal van 1 tot 4?

#	Answer	%	Count
1	1, niet meegenomen	18.18%	4
2	2	31.82%	7
3	3	18.18%	4
4	4, volledig op elkaar afgestemd	31.82%	7
	Total	100%	22

Q1.37 - 27. In hoeverre is sprake van onderlinge afstemming tussen de strategie van het fonds en IT, zodat IT een optimale bijdrage levert aan het behalen van de organisatiedoelstellingen?

#	Answer	%	Count
1	1, niet meegenomen	31.82%	7
2	2	27.27%	6
3	3	27.27%	6
4	4, volledig op elkaar afgestemd	13.64%	3
	Total	100%	22

Q1.38 - 28. Maakt uw fonds gebruik van de DNB Good Practice informatiebeveiliging self-assessment die in 2019 is uitgebracht en heeft u dit assessment in de afgelopen drie jaar uitgevoerd

#	Answer	%	Count
1	Ja	40.91%	9
2	Nee	59.09%	13
	Total	100%	22

Q1.39 - 28.1. In het self-assessment zijn 58 verschillende controls waar pensioenfondsen aan moeten voldoen. Deze controls worden getoetst op een volwassenheidsniveau van 1 tot 5. Weet u van de onderstaande controls welk volwassenheidsniveau door uw fonds in het self-assessment is ingevuld.

#	Question	1	2	3	4	5	weet ik niet
1	4.1 IT-riskmanagement framework	0.00%	11.11%	22.22%	55.56%	0.00%	11.11%
2	4.2 Risk assessment	0.00%	11.11%	11.11%	66.67%	0.00%	11.11%
3	4.3 Maintenance and monitoring of a risk action plan	0.00%	11.11%	33.33%	44.44%	0.00%	11.11%
4	9.3 Employee awareness	0.00%	22.22%	44.44%	22.22%	0.00%	11.11%
5	14.1 Monitoring and reporting of service level achievements (SLA)	0.00%	22.22%	33.33%	33.33%	0.00%	11.11%
6	14.2 Supplier risk management	0.00%	11.11%	55.56%	22.22%	0.00%	11.11%
7	16.3 Internal control at third parties	0.00%	22.22%	33.33%	33.33%	0.00%	11.11%
8	19.2 Vulnerability management	0.00%	11.11%	44.44%	22.22%	0.00%	22.22%
9	19.3 Application life cycle management	0.00%	22.22%	44.44%	11.11%	0.00%	22.22%
10	22.1 Penetration testing and ethical hacking	0.00%	11.11%	33.33%	33.33%	0.00%	22.22%

Q1.40 - 29. Wordt binnen het fonds gebruik gemaakt van op scenario gebaseerde incident training waarbij het bestuur actief deelneemt? Incident training is een training om medewerkers binnen een organisatie te leren hoe ze zich kunnen voorbereiden op het afhandelen van en reageren op (beveiligings)incidenten in mogelijke scenario's

#	Answer	%	Count
1	Ja	4.55%	1
2	Nee	95.45%	21
	Total	100%	22

Q1.41 - 29.1. Is bij de incident training ook aandacht gegeven aan scenario's over actuele cyberdreigingen

#	Answer	%	Count
1	Nee	0.00%	0
2	Ja	100%	1
	Total	100%	1

Q42 - 30. Wordt binnen het fonds gebruik gemaakt van op scenario gebaseerde continuïteitstraining waarbij het bestuur actief deelneemt? Continuïteitstraining is een training om medewerkers binnen een organisatie te helpen effectief te reageren op mogelijke scenario's waarbij het doel is om de bedrijfscontinuïteit te waarborgen?

#	Answer	%	Count
1	Ja	0.00%	0
2	Nee	100%	22
	Total	100%	22

Q43 - 30.1. Is bij de continuïteitstraining ook aandacht gegeven aan scenario's over actuele cyberdreigingen

#	Answer	%	Count
1	Ja	0.00%	0
2	Nee	0.00%	0
	Total	100%	0

Q1.44 - 31. Wordt binnen het fonds gebruik gemaakt van ketentesting waarbij het fonds samen met een uitbestedingspartner samenwerkt om informatiebeveiliging of cybersecurity tests of trainingen te doen?

#	Answer	%	Count
1	Ja	18%	4
2	Nee	82%	18
	Total	100%	22

Q60 - 31.1 Met welke uitvoerders voert u deze ketentesting uit?

#	Answer	%	Count
1	Bestuursbureau	37.50%	3
2	Pensioenadministratie	50.00%	4
4	Vermogensbeheer	12.50%	1
6	Anders, namelijk	0.00%	0
	Total	100%	8

Q1.45#1 - 32. Wordt binnen de verschillende pensioendomeinen van het fonds gebruik gemaakt van phishing oefeningen - Ja / Nee

#	Question	Ja		Nee		Total
1	Pensioenbeheer domein	36.36%	8	63.64%	14	22
2	Vermogensbeheer domein	27.27%	6	72.73%	16	22
3	Bestuursomgeving domein	40.91%	9	59.09%	13	22

Q1.46 - 33. Is uw fonds aangesloten bij de Pensioenfonds ISAC om huidige ontwikkelingen en risico's op het gebied van informatiebeveiliging en cybersecurity te volgen en te delen met elkaar? Een pensioenfonds-ISAC is een informatie-uitwisselings- en analysecentrum of die een centrale bron biedt voor het verzamelen van informatie over cyberdreigingen voor de pensioen sector)

#	Answer	%	Count
1	Ja	0.00%	0
2	Nee	31.82%	7
3	Wel van gehoord, maar niet aangesloten	31.82%	7
4	Nog nooit van gehoord	36.36%	8
	Total	100%	22

Q1.47#1 - 34. Bent u bekend met huidige technologische ontwikkelingen op het gebied van blockchain, kunstmatige intelligentie en cloud oplossingen

#	Question	1		2		3		4		Total
1	Blockchain	9.09%	2	77.27%	17	9.09%	2	4.55%	1	22
2	Kunstmatige intelligentie	9.09%	2	68.18%	15	18.18%	4	4.55%	1	22
3	Cloud oplossingen	0.00%	0	31.82%	7	59.09%	13	9.09%	2	22

Q1.48 - 37. Wordt voor de classificatie van de IT-risico's van het fonds gebruikt gemaakt van de methode: risico = kans × impact of wordt gebruik gemaakt van op een scenario gebaseerde methode?

#	Answer	%	Count
1	Kans × Impact	59.09%	13
2	Scenario gebaseerd	0.00%	0
3	Overig, namelijk	0.00%	0
4	combinatie van kans × impact en scenario gebaseerd	40.91%	9
	Total	100%	22

D. Validation of the survey results

Vragen + antwoorden (samengevat)

1. Uit de survey kwam naar voren dat 61% van de ondervraagde pensioenfondsen de DNB Good Practice IB & Cybersecurity niet (volledig) implementeert. Vanuit welke overweging heeft uw fond wel of niet de Good Practice geïmplementeerd?
    a. (2/3) te weinig expertise en kennis aanwezig om hier voldoende invulling aan te geven.
    b. (2/3) Uitbestedingspartners (voornamelijk PUO) heeft dit gedaan en rapporteert hieraan terug over ons. Dit is voldoende voor ons
2. Uit de survey kwam naar voren dat 96% van de ondervraagde pensioenfondsen geen gebruikt maakt van scenario gebaseerde oefeningen (met hun uitbestedingspartners). Bent u hiermee bekend en vanuit welke overweging maakt uw fonds wel of geen gebruik van scenario gebaseerde testen?
    a. (2/3) Nog nooit van gehoord
    b. (1/3) Verkrijgt periodiek informatie van PUO, maar is voornamelijk op IT-risks gebaseerd en niet op informatie en cybersecurity.
3. Uit de survey kwam naar voren dat geen enkele van de ondervraagde pensioenfondsen direct dan wel indirect is aangesloten bij de Pensioen-ISAC, om als pensioenfonds van informatie te worden voorzien omtrent informatiebeveiligings- en cybersecurity risico's. Hoe geeft uw fonds invulling aan het verkrijgen van informatie over informatiebeveiligings- en cybersecurity risico's binnen uw IT keten?
    a. (3/3) Niet van gehoord, enige vorm van informatie komt vanuit de uitbestedingsrelaties.
    b. (2/3)Bestuursleden vinden het een lastig onderwerp en gaat snel te diep.
4. Uit de resultaten komt naar voren dat ongeveer de helft van de ondervraagde pensioenfondsen geen inzicht heeft in de IT-ketens die voor het fonds zijn ingericht. Hoe verkrijgt uw fonds inzicht in de IT-ketens? Onder de IT-keten vallen onder meer de IT-infrastructuur, de applicaties die door uw uitbestedingspartners gebruikt worden en de locaties waar uw data is opgeslagen.
    a. (1/3) Wordt summier verkregen van hun PUO, niet van assetmanagement.
    b. (2/3) Vooral op basis van ISAE 3402 rapportage. Of dit de volledige IT-infrastructuur dekt weten pensioenfondsen niet.
5. Uit de resultaten van de survey komt naar voren dat minder dan 30% van de ondervraagde pensioenfondsen verantwoordingsrapportages krijgen over informatiebeveiliging en cybersecurity. Hoe geeft uw fonds invulling aan het verkrijgen van genoeg informatie om uw informatiebeveiligings- en cybersecuritymaatregelen te kunnen monitoren en valideren?
    a. Verantwoordingsrapportages worden vooral geleverd vanuit de uitbestedingsrelaties.
    b. Pensioenfondsen hebben het idee dat ze "slechts" een van de zoveel pensioenfondsen zijn die de uitbestedingspartij bediend en daarom minder geneigd is om specifieke verantwoordingsrapportages op te vragen.
6. Uit de resultaten van de survey komt naar voren dat 40% van de ondervraagde pensioenfondsen IT-deskundigheid en ervaring heeft meegenomen in de geschiktheidseisen van pensioenfonds bestuursleden. Hoe geeft uw fonds invulling aan geschiktheidseisen omtrent IT?

    a. (1/3) Niet meegenomen, wel van bewust dat er geen deskundigheid aanwezig is en daarom afspraken gemaakt met bedrijven die hier invulling voor het fonds aan kunnen geven.
    b. (2/3) Zit summier verwerkt in de geschiktheidsplannen
7. Uit de resultaten komt naar voren dat 60% van de ondervraagde pensioenfondsen kennis en ervaring omtrent IT gewaarborgd heeft binnen het fonds. Hoe geeft uw fonds invulling aan het (onderhouden van) kennis en ervaring omtrent IT.
    a. (1/3) ad-hoc ingeschakeld.
    b. (2/3) periodieke cursussen zelf en soms vanuit de PUO georganiseerde bijeenkomsten.
8. Uit de resultaten van de survey komt naar voren dat ongeveer de helft van de ondervraagde pensioenfondsen hun beleidsdomeinen (IT, uitbesteding en Integraal risicomanagement) niet volledig op elkaar hebben afgestemd. Op welke wijze heeft uw fonds deze drie beleidsdomeinen afgestemd op elkaar?
    a. (1/3) weinig, er is geen cohesie tussen beleidsdomeinen.
    b. (2/3) wordt beschreven en op sommige vlakken aandacht aan gegeven, nog niet volledig op elkaar afgestemd. Komt vooral dat er andere prioriteiten maar aandacht krijgen.
9. Uit de resultaten van de survey komt naar voren dat ongeveer 75% van de ondervraagde pensioenfondsen een IT-risico appetite heeft geformuleerd voor haar verschillende IT-domeinen. Hoe heeft uw fond invulling gegeven aan het opstellen van uw IT-risico appetite?
    a. (3/3) op basis van een risicoanalyse.
    b. (2/3) op basis van een BIV-classificatie.
    c. (1/3) risk appetite wordt jaarlijks geupdated.

Het verbeter model

Aan de hand van de verkregen resultaten uit de survey zijn verschillende verbeteringen bedacht om het huidige niveau van informatiebeveiliging en cybersecurity van pensioenfondsen te verhogen. Deze verbeteringen zijn verwerkt in een verbeter model. Dit model kan gebruikt worden als supplement op het DNB Good Practice framework om het niveau van informatiebeveiliging en cybersecurity van het fonds naar een hoger niveau te tillen. Het verbeter model adresseert gevonden verbeterpunten vanuit de survey en benadrukt aspecten waar de DNB Good Practice laag op scoorde.

De randvoorwaarden:

1. De pensioenfondsen moeten een geschiktheidsbeleid hebben opgesteld waarin IT-geschiktheidseisen en ontwikkel plannen zijn opgenomen.
2. Het Good Practice-framework is geïmplementeerd binnen het fonds.
3. Voor de IT-domeinen pensioenadministratie en vermogensbeheer dient door het pensioenfonds sectorale dreigingsinformatie te worden verkregen. Binnen het IT-domein bestuur omgeving wordt het pensioenfonds door haar IT-dienstverlener proactief geïnformeerd over relevante IT-dreigingen.
4. Contractuele afspraken zijn gemaakt tussen pensioenfonds en uitbestedingsrelatie omtrent verantwoordingsrapportages over de geïmplementeerde maatregelen van informatiebeveiliging en cybersecurity.

5. Pensioenfondsen dienen een beleidskader te hebben voor IT, informatiebeveiliging en cybersecurity.
6. Het pensioenfonds heeft een kwalitatieve IT-risico appetite geformuleerd die is afgestemd met de strategie van het fonds én waarbij de eisen voor de aspecten vertrouwelijkheid, integriteit en beschikbaarheid zijn geformuleerd.
7. De verschillende beleidsdomeinen (IT, uitbesteding en integraal risicomanagement) zijn op elkaar afgestemd en worden periodiek herzien en geactualiseerd.

Vragen over het verbeter model Inclusief antwoorden.

5. In hoeverre zou dit model in combinatie met de gestelde randvoorwaarden uw fonds kunnen helpen meer grip te krijgen op informatiebeveiliging en cybersecurity. Op een schaal van 1 tot 10?

Pension fund 1	Pension fund 2	Pension fund 3
7	8	8

Pensioenfonds 1 is een klein fonds en vind het lastig om aan de randvoorwaarden te voldoen.

6. In hoeverre zou uw fonds dit model kunnen toepassen binnen het bestaande risico raamwerk van het fonds op een schaal van 1 tot 10?

Pensioenfonds 1	Pensioefonds 2	Pensioenfonds 3
8	8	8

Het model is niet volledig nieuw voor de pensioenfondsen en skuit goed aan bij hun huidige IRM raamwerk.

7. In hoeverre zou dit model uw fonds kunnen helpen bij het verhogen van het bewustzijn omtrent informatie en cybersecurity voor de pensioenfonds bestuurders op een schaal van 1 tot 10?

Pensioen fonds 1	Pensioen fonds 2	Pensioen fonds 3
8	8	8

8. Zijn er aspecten die nog missen binnen het model of die verbeterd kunnen worden?
    a. Proportionaliteit beter in verwerken of een soort “light” variant van maken voor kleine pensioenfondsen.
    b. Een trigger erin verwerken waarmee het bestuur de huidige staat van informatie en cybersecurity mee kan monitoren (zoals de dekkingsgraad percentage).

E. ICS improvement model activities

Phase	Inventory and setup (Plan)
Activity	A1 Identification of the IT landscape
Deliverable	IT landscape overview
Prerequisite	4, 6
Description	Pension funds must make the contractual agreement with their managed service provider that the pension fund periodically obtains an overview of the IT landscape of the service provider. The IT landscape overview must include: - Used applications per outsourced service - Critical outsourced services - Third party applications - Location of stored data Based on the IT landscape overview the pension fund can perform the IT risk assessment as described in the DNB Good Practice framework.

Phase	Inventory and setup (Plan)
Activity	B1 Awareness and training plan
Deliverable	Awareness and training plan
Prerequisite	6
Description	The pension fund must include the following topics in addition to their current awareness and training plan. - Scenario based testing and that simulate actual information and cybersecurity attacks - Role based information and cybersecurity training - Information and cybersecurity training and exercises with their managed service providers - A combination of theoretical and practical information and security exercises. - Active participation of pension fund board members

Phase	Setup and deployment (Do)
Activity	A2 Ensuring sufficient evidence
Deliverable	Accountability reports with the correct scope and depth
Prerequisite	4
Description	The pension fund must have defined in the SLA with their managed service providers to obtain evidence of the implemented information and cybersecurity controls. This phase focusses on obtaining and ensuring that this evidence is delivered and has the correct depth and scope.

Phase	Setup and deployment (Do)
Activity	A3 Continuous threat analysis
Deliverable	Threat analysis report
Prerequisite	5
Description	The pension fund performs continuous threat analysis for all the relevant IT domains. The pension fund must ensure that they are periodically updated with regard to important developments and possible information and cyber risks and they must take action on the basis of their IT risk appetite. Threats that are not immediately tackled can be added to the IT risk improvement plan. The threat analysis reports can also provide input for the scenario-based testing and training.

Phase	Setup and deployment (Do)
Activity	B2 Scenario based testing and training exercises
Deliverable	Scenario report
Prerequisite	5
Description	The awareness and training exercises defined in the plan phase will be performed this phase. The awareness and training exercises must be documented for the monitoring and evaluation phase and to make it demonstrable that pension fund board members are actively participating.

Phase	Setup and deployment (Do)
Activity	B3 IT training and education
Deliverable	Scenario report
Prerequisite	1
Description	Based on the IT requirements stated in the suitability plans and the development plans pension fund board members must follow IT training and education to increase the knowledge regarding IT related topics, including information and cybersecurity. In order to gain knowledge regarding the different IT domains, the pension fund must cooperate with their managed service providers for IT related knowledge trainings. The training and education for each of the board members must be documented for the monitoring and evaluation if the IT requirements are met.

Phase	Monitoring and verification (check)
Activity	A4. Review accountability reports
Deliverable	Accountability reports
Prerequisite	4
Description	The pension fund has made agreements regarding the accountability reports the pension fund obtains for the monitoring and validation of the implemented DNB Good Practice controls. The pension fund must validate that the accountability reports have the correct scope and depth for the monitoring of the DNB Good Practice controls

Phase	Monitoring and verification (check)
Activity	A5. Review accountability reports
Deliverable	DNB Good Practice self-assessment report
Prerequisite	2
Description	The pension funds use the DNB Good Practice self-assessment to validate the maturity level of their implemented controls. The self-assessment can be filled in with the evidence provided with the accountability reports and in cooperation with the managed service provider. If evidence is missing or an implemented control is not at the required level, the pension fund takes immediate action to resolve this, or the issue will be documented in the IT improvement plan for the next cycle. za

Phase	Monitoring and verification (check)
Activity	B3. Monitoring awareness and training
Deliverable	Awareness and training progress report
Prerequisite	1
Description	The results of the awareness and training is checked and compared to the objectives stated in the awareness training plan. The individual training plan of the pension fund board members are checked if the predefined goals regarding IT knowledge are met.

Phase	Evaluation and adjustment (act)
Activity	A6. IT risk improvement plan
Deliverable	IT risk improvement plan
Prerequisite	
Description	Based on the results of the DNB Good Practice self-assessment and the accountability reports possible controls can be identified that are not at the required level. In order to improve the current level and based on the importance of the control immediate action can be taken to resolve it or it can be recorded in the IT risk improvement plan to be improved next cycle. In addition, the results of the continuous threat analysis will be incorporated into the IT risk improvement plan.