Cyber vulnerabilities and IT risk management in the Dutch housing association sector.

Towards a 'privacy & information security' framework.

Thomas IJpelaar
STUDENT NUMBER: 2002835

THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION MANAGEMENT
TILBURG SCHOOL OF ECONOMICS AND MANAGEMENT
TILBURG UNIVERSITY

Thesis committee:

Supervisor: Dr. Ali Pirannejad
Second Reader: Catherine Ma
Company Supervisor: drs. Martijn Videler

Tilburg University
Tiburg School of Economics and Management
Department of Management
Tilburg, The Netherlands

Januari 2023

Abstract

At the beginning of 2022, eight Dutch housing associations became victims of a cyber attack. During the hack, privacy & information security got compromised and data about the organization and its tenants leaked. This research investigates how IT risk management could help Dutch housing associations to manage their cyber vulnerabilities. To explore how privacy & information security should be considered when discussing IT risk management in the Dutch housing association, a multiple-case study on five housing associations is done. Furthermore, expert interviews are conducted to evaluate the different aspects further. The results show that it is important to keep in mind the people, processes, and technology within a housing association when evaluating how IT risk management is used in a housing association. Furthermore, for housing associations to get a grip on the IT risks, a structured way of examining cyber threats and their impact on the organization and a sector-wide approach to these threats will positively influence the sector's ability to manage the cyber vulnerabilities. Moreover, there is a need to strongly embed IT risks in risk management and the enclosure of a continuous way of the IT risk management process to ensure privacy & information security. This research moves toward a Dutch housing association sector-specific 'privacy & information security' framework. Providing a clear overview of the different factors that are important for IT risk management in the Dutch housing association sector.
Keywords: *IT risk management; Privacy and information security; Cyber vulnerabilities; Cyber security; the Dutch housing association sector.*

T. IJpelaar

Academic summary

The Dutch housing association sector provides affordable housing services to a significant part of the Netherlands. To fulfill their services and to protect their tenants and own organization, privacy and information security play an important role in the sector. IT risk management could be used to improve the sector's ability to manage cyber vulnerabilities. However, regarding digital vulnerabilities, risk management is still in its infancy in the Dutch housing association sector. Both 'privacy and information security' and 'risk management' are well-studied variables in general; however, their effect in the Dutch housing association sector shows a research gap for this thesis to fill. This thesis aims to address the gap in the literature by discovering what elements should be included in the sector-specific 'privacy & information security' framework. Therefore exploratory research is conducted to answer the main research question: *"How could Dutch housing associations use IT risk management to manage their cyber-vulnerabilities?"*. This objective is achieved by collecting data through a literature review, case-study research, and expert interviews. Semi-structured interviews were used to gather data from the cases and experts in the Dutch housing association sector context. The data analysis is carried out by systematically coding the raw data multiple times, creating a data analysis structure providing the codes, main themes, and topics of interest. The research findings show that for Dutch housing associations to use IT risk management to manage their cyber-vulnerabilities, several areas need focus. At first, external developments, evolving cyber threats, security assistance, and legislation must be considered. Furthermore, people, processes, and technology should be included when considering the internal variables of housing associations on the topic of privacy & information security. At last, the continuous evaluation of IT risks and the IT management process helps the Dutch housing associations manage their cyber vulnerabilities. From an academic perspective, these findings are relevant because of the systematic review of privacy, information security, and IT risk management within the Dutch housing association sector. The discovered elements of the sector-specific framework will benefit the research area of interest, the Dutch housing association sector, and contribute to the academic world. However, further studies should be undertaken to evaluate the 'privacy & information security' framework and improve the overall credibility of the framework. Sectors that are similar to the Dutch housing association also present an interesting area for future research, as best practices could be observed and their potential to the Dutch housing association sector evaluated.

Managerial summary

The Dutch housing association sector is essential in providing affordable homes in Dutch society. Moreover, housing associations provide the service of having affordable homes to vulnerable groups in society. For Dutch housing associations to offer their services, it is vital to protect the personal data of their tenants. However, the cyber threat landscape is ever-evolving, threatening Dutch housing associations' privacy and information security. Therefore, the Dutch housing association sector must put privacy and information security on the agenda to best defend themselves against cyber vulnerabilities. This research explores how IT risk management could best be used in the Dutch housing association sector and what factors are essential to keep in mind when managing IT risk to ensure privacy and information security. Moreover, this research moves towards a clear framework that emphasizes IT risk management within the Dutch Housing Association sector to strengthen privacy and information security within organizations that are active in this sector. The main findings of this research exploration of the Dutch housing association sector and IT risk management comprise several areas of interest. First, the internal variables important to IT risk management consists of people, processes, and technology. Particular attention should be given to the organizational-wide feeling of responsibility toward IT risk management, further focusing on the awareness of all employees on the topic of privacy & information security. Secondly, sector-wide cooperation between Dutch housing associations on sharing knowledge and experiences would benefit the entire sector's cyber resilience. It would help to keep individual housing associations aware of the different evolving cyber threats and their possible impact on their organization, making the IT risks they face manageable. The third area of interest is the enclosure of privacy & information security in the risk management process of housing associations, creating a continuous way of dealing with IT risk. The NIST cyber security framework, or the ISO 27005, provide helpful tools for housing associations to grab hold of their IT risk management and secure against cyber vulnerabilities. This study presents the important variables for the Dutch housing association sector to use IT risk management. However, further research is needed. Further research into the proposed sector-specific framework should be done for the framework to be of true value to the sector. Research the individual aspects mentioned in the 'privacy & information security' framework and further testing of the framework due to future research. Furthermore, best practices from other sectors on IT risk management, privacy, and information security to defend against cyber vulnerabilities and how these best practices could benefit the Dutch housing associations sector could provide exciting areas for future research.

T. IJpelaar

Acknowledgement

I would like to thank my supervisor, Dr. Ali Pirannejad for his guidance and support throughout the entire thesis process. Furthermore, I would like to thank my supervisor from VVA-informatisering, drs Martijn Videler, for his advice and support throughout the process and for the opportunity to combine writing a thesis with gaining practical experience. Last but not least, I would like to thank my family and friends for their support.

"Ideas are like rabbits. You get a couple and learn how to handle them, and pretty soon you have a dozen"
- John Steinbeck

Contents

Cyber vulnerabilities and IT risk management in the Dutch housing association sector. Towards a 'privacy & information security' framework.

Thomas IJpelaar

1 Introduction

1.1 Problem indication

In their report on Global Risks in 2022, the World Economic Forum noticed the widespread dependency on increasingly complex digital systems. This growing dependency on digital systems has shifted how many societies function. More so, it allowed the adoption of devices and platforms that allow sensitive data to be shared with third parties, like service providers. Together with the ever-growing demand for new technological capabilities, the ever-changing digital landscape exposes us all to harmful digital and cyber risk (World-Economic-Forum, 2022). According to the WEF report, "Cyber security failure" ranks as a top five risk in Europe and is among the top 10 risks that have worsened most since the start of the COVID-19 crisis.

Beaman et al. (2021) concluded that "the COVID-19 pandemic has led to an increase in the rate of cyberattacks" (p.1). According to Beaman et al. (2021), cybercriminals are constantly exploring different ways to spread ransomware, and approaches like social engineering attacks like phishing attacks keep evolving. An annual study done by Sophos (2022) found that the proportion of organizations impacted by ransomware doubled in twelve months, from a third in 2020 to two-thirds in 2021. From the 150 IT professionals of mid-sized companies based in the Netherlands who took part in the Sophos study, 69% of them replied with a yes when asked if their organization has been hit by ransomware in the last year. Showing the ever-growing cyber-security challenges that organizations have to face.

The main Dutch counter-terrorism unit, the 'National Coördinator Terrorismebestrijding en Veiligheid (NCTV),' assesses Cyber-risks in the Netherlands and provides guidance to make strategic choices to better protect the Dutch society against cyber-attacks. The NCTV also noticed an increase in cyber risks, with different actors becoming more active, like nation-states, hacktivists, and organized crime. In their latest report on cybersecurity in the Netherlands, the NCTV states that the unbalance between cyber-threats and cyber-resilience increases the risk of disruption in the Dutch society (ministry-of Justice & Security, 2022). The NCTV provides six strategic subjects relevant to the Netherlands's digital safety in the upcoming four to six years. One of

those strategic subjects is risk management because of the lack of a structural place for cyber-risks in the risk management of many organizations, sectors, and countries (ministry-of Justice & Security, 2022).

On the 27th of march 2022, The Sourcing Company (TSC), a company providing online cloud-based workspaces to their customers (Company, 2022), became a victim of a Conti ransomware attack (Sanders, 2022)(Verlaan, 2022). Furthermore, some of TSC's customers fell victim as a result of the TSC hack as well, including eight housing associations throughout the Netherlands. Next to the downtime of their websites and all of their IT systems, personal data has also leaked. Among the personal data are names, phone numbers, addresses, and bank accounts of thousands of tenants (Groenendijk, 2022)(Verlaan, 2022). The criminal syndicate behind the attack eventually released the leaked personal data on the dark web because the victims wouldn't pay the ransom of 15 million euros asked (Monternie, 2022). In the same month, another Housing Association called DeltaWonen got victim of another hacking attack (Engelaar, 2022). The hackers gained access to an employee's email account and could steal the personal data of DeltaWonen's clients. The attacked housing associations are still busy recovering from the cyber-attacks. There are still many lessons to be learned about privacy and information security within the housing associations sector. More specifically, how housing associations could better arm themselves against future cyber vulnerabilities.

A sector-specific approach to cyber security is needed to better prepare housing associations against cyber vulnerabilities in the future. Securing information is a challenge, and to better prepare the housing association sector, the privacy, and information security factors could be scoped out from the risk management approach. Risk management helps to create a systematic way to make a trade-off between the benefits (e.g., safety, security, cyber-resilience) and the costs (e.g., investments, reduction of flexibility, reduction of usability) within the scope of the housing association sector.

1.2 Problem Statement

Regarding digital vulnerabilities, risk management is still in its infant stage, according to the NCTV (ministry-of Justice & Security, 2022). With the acceleration of digital transformation by using mobile devices, social media, cloud services, and the Internet of Things, cybersecurity has become a key concern in risk management (Lee, 2021). In his paper on cybersecurity Lee (2021) wrote that a multi-layer approach is needed for cyber risk management. With strong attention to technical and human aspects, taking into account the cybersecurity trends, new threat methods and techniques, existing cybersecurity frameworks, and legislations.

In a paper by Zakhour & Vasudevan (2021) written on behalf of Atos, a global leader in digital transformation (Atos, 2022), a prediction on the top 7 cybersecurity threats for 2022 is given. Cyber threats like ransomware, third-party, supply chain or cloud threats are mentioned. Zakhour and Vasudevan (2021) state that the cyber threat landscape is moving fast. Every year, companies must evolve and adapt their defenses to protect against the next wave of large cyber threats they will face.

With the hack of the TSC (Sanders, 2022) and the violation of the confidentiality, integrity, and availability of data and information within their systems, it became clear that companies within the housing association sector in the Netherlands should keep evolving and keep adapting their defenses to better protect themselves from the continuously evolving cyber threats. One way for Dutch housing associations to improve their cyber defenses and resilience is to integrate cyber risks, or IT risks, into their risk management, as risks management is still in its infants stage when it comes to digital vulnerabilities (ministry-of Justice & Security, 2022).

Further research on IT risks and how they are managed in the housing association sector is needed. This research explores how IT risk management could help the Dutch housing association sector manage its cyber vulnerabilities better to secure privacy & information in their organization. Furthermore, this thesis moves toward a sector-specific framework that could help the Dutch housing association to manage the ever-evolving cyber-risks. To move towards a theoretical framework, an exploration of what aspects are essential and how they relate to each other within the context of the Dutch housing association sector is conducted. Moreover, the framework will be based on existing cyber security frameworks, legislation, theory on cyber security and risks management and privacy and information security, new threat methods and techniques, the human aspects, and specific aspects of the Dutch housing association sector.

1.3 Research Question

In line with the problem indication and problem statement, the following main research question has been formulated:
"How could Dutch housing associations use IT risk management to manage their cyber-vulnerabilities?"

To deal with the main research question, the following sub-questions have to be answered:

1. What are the internal variables when it comes to organizational cyber-vulnerabilities in the Dutch Housing Association Sector?

The internal variables of cyber vulnerabilities are important in this research when discussing IT risk management. To further understand cyber vulnerabilities' impact on the Dutch housing association sector, we must first discover what internal variables influence the organizations. Furthermore, we dive into the topic of cyber security, understanding what measures organizations can take to secure themselves against cyber threats. The research inspects how housing associations currently organize their cyber security to manage cyber vulnerabilities. Also, the human factor will be considered, taking a look at, for example, the effect management and employees can have on the cyber resiliency of a firm.

2. What are the external developments when it comes to cyber-vulnerabilities in the Dutch housing association sector?

External developments concerning cyber vulnerabilities are important variables in this research. To further understand cyber-vulnerabilities' impact on the Dutch housing association sector, we must first discover what external developments influence the

organizations. Furthermore, we dive into the topic of cyber threats. Taking a deeper understanding of the evolving cyber-threat landscape, the main risks for the Dutch housing association sector, and the external cyber threats- and- security developments. Furthermore, the external effects of legislation and regulations on an organization are considered.

3. To what extent is IT risk management used in the Dutch housing association sector to manage cyber-vulnerabilities?

To further understand how risk management methods are used to manage IT risk, the field of IT risk management in the Dutch housing association sector is being evaluated. We must first discover what the risk management process looks like, reviewing the different policies, procedures, and technologies used in the sector to manage the cyber-vulnerabilities.

4. What is the function of IT risk management in protecting the privacy and information security in Dutch housing associations, with regards to managing cyber vulnerabilities?

To understand how IT risk management could be used to better secure privacy & information in the context of the Dutch housing association sector, the cohesion between the two topics is evaluated. Furthermore, the literature on privacy & information security on the topic is presented to lay the foundation for the Dutch housing association sector-specific framework.

1.4 Research Approach

The research is conducted through qualitative research. First, a literature review is conducted to gain valuable insights, theories, and information. The data used for the literature review is secondary data related to the main concepts or variables, being: 'privacy and information security,' 'the Dutch housing Association Sector,' '(IT-)Risk Management,' 'cyber-threats,' 'cyber-security' and 'cyber-security frameworks.' The secondary data sources used in the literature part of this research are primarily from Information Management related journals obtained via the Tilburg University Library. To safeguard the reliability of the literature review, the most used scientific journals are the MIS Quarterly, Management Science, INFORMS Journal on Computing, Information Systems Research, and other top journals from within the field of Information Management and related topics. Furthermore, the research done by Levy & J. Ellis (2006) on a systems approach to conduct an effective literature review in support of information systems research' provides the framework used for the literature data processing. Literature gathering and screening, processing, and writing are the steps taken to create an effective literature-based foundation for this proposed research.

Next to the literature review that provides a start for this research, the data collection is conducted via case-study research and expert interviews (DiCicco-Bloom & Crabtree, 2006). Case-study research is undertaken to investigate the different topics further and address the gaps in the literature regarding the housing association sector. In the case-study research, five separate cases (Yin, 2014) are selected from within the Dutch housing association sector. The case-study research will help provide relevant

insights into the Dutch housing association sector. Furthermore, expert interviews are conducted to gain further insights into the Dutch housing association sector and the different concepts 'of privacy and information security,"(IT-)Risk Management,' 'cyber-threats,' 'cyber-security,' and 'cyber-security frameworks.' The validity, purposefulness, and insights generated from the interviews have more to do with the information-richness of the cases selected than with the sample size (Crabtree & Miller, 1999). According to Crabtree & Miller (1999), it is important to have clear criteria to select the right participants. The interviewees meet specific criteria and are therefore selected; the requirements are further elaborated in chapter three. The literature review, case-study research, and expert interviews help achieve the thesis's primary goal, which is to answer the main research question with the help of a privacy & information security framework.

1.5 Thesis Structure

The structure of this thesis is based on answering the sub & main research question through case-study research complemented with expert interviews. The first chapter introduces the different topics, problems, and the need for a solution. The second chapter provides the theoretical framework for this research, reviewing the literature on the main topics. Chapter three further explain the research methodology used in this thesis. In chapter four, the results of the data analysis are presented. After the presentation of the results, those results are discussed and compared with the theory in chapter five. Furthermore, the discussion provides the answers to the sub-research questions. The conclusion will summarize the findings and the answer to the main research question. Along with the discussion and conclusion, chapter five presents the limitations of this research and recommendations for future research. The bibliography and appendices will follow the last chapter.

2 Theoretical framework

In this chapter, a selective, in-depth, and critical literature review is given on the topics of the Dutch Housing Association Sector, the cyber threat landscape, IT-Risk Management, and privacy & information security. The concepts and relations between the subjects are discussed and evaluated based on existing literature. At the end of the chapter, a summary will be provided.

2.1 Dutch Housing Association Sector

2.1.1 History and goals of Dutch housing associations

In the year 2021, there were around 8 million houses in the Netherlands (CBS, 2021). About a third of those houses, 2,4 million, are rented out by around 300 different Dutch housing associations with a total of approximately 25.000 employees (WerkenAanWonen, 2022). The housing association sector found its origins at the beginning of the twentieth century when local governments became heavily involved in the Dutch rental housing market, emphasizing the lower and middle end of the market (Koopman et al., 2009a). Because of the growing costs of public housing during the 1990s, the (local) governments were forced to abandon their direct control over the public housing sector, and the Dutch housing associations became self-organized non-profit organizations. The goal of the housing association sector is combining public tasks and meeting the market demand, with the responsibility to maintain a high quality of life in neighborhoods and cooperation with civil society organizations (ministry of the Interior & Relations, 2021). Furthermore, the Dutch housing associations sector provides affordable housing to low-income tenants (Koopman et al., 2009b). To further commit the housing association sector to their given tasks, Aedes, a national network organization promoting the interest of the housing associations in the Netherlands, in June 2022, made an arrangement with the Ministry of the Interior and Kingdom Relations. Agreeing on, for example, the improvement in quality of life in the neighborhoods, the construction of 300.000 new houses, and the improvement of sustainability in all houses rented out by housing associations (ministy-of-the-Interior-and Kingdom-Relations & Aedes, 2022). These agreements between the government and dutch housing associations show the combination of public tasks and meeting market demands and, together with their place in society, display that housing associations in the Netherlands are the unique link between the state, civil society, and the economic market place (Helderman, 2007).

In their book on 'performance measurements in the Dutch social rented sector' Koopman et al. (2009a) wrote that housing associations started using private sector approaches due to the drive towards more professional standards. Resulting in, for example, the use of outsourcing, the use of asset management, the internal and external supervision of the performance of housing associations, and the creation of sector-specific performance measurements. According to Koopman et al. (2009b), the following tasks are essential for the performance measurement of housing associations:

1. *"To guarantee the financial continuity of the housing association."* (p.5)
2. *"To provide affordable housing to low-income tenants (households with a below-modal income)."* (p.5)

3. *"To maintain the quality of the housing stock."* (p.5)
4. *"To ensure tenant empowerment by giving tenants a say in policy matters and housing management."* (p.5)
5. *"To increase and maintain the quality of life in the area surrounding the dwellings."* (p.5)
6. *"To provide joint housing-and-care arrangements."* (p.5)

The organizational structure of the Dutch housing associations took the form they have today to best fulfill the tasks described by Koopman et al. (2008).

2.1.2 Dutch housing associations as an organization

The CORA is developed in the sector to further explain the organizational structure in Dutch housing associations. The CORA 3.0 is a rapport on the management and architecture of housing associations in the Netherlands. Describing the housing associations' primary and supporting business processes (netwIT-and-FLOW-and Aedes, 2011). The CORA 3.0 also shows that IT services are part of the supporting processes in housing associations. Furthermore, it shows that the executive board directs the entire organization of primary and supporting processes. An overview of primary and supporting processes in Dutch housing associations can be found in appendix B, figure 12 and figure 13. Two departments are further explained, because of their role in the housing association. The information and Automation department (I&A) and the Control department. The I&A department in a housing association is responsible for managing and maintaining the organization's information systems and technology infrastructure (CORA, n.d.). The Control department in a housing association is responsible for monitoring and adjusting the implementation of plans to which a housing association aims to achieve its goals. Furthermore evaluating and reporting periodically on the organizational performance, and assessing whether the organization remains in control of the performance (*CORA*, n.d.).

Next to the organizational structure of Dutch housing associations, the housing associations are organizations with many interrelated and interdependent technical and human factors in place. In research by Dhillon et al. (2021), socio-technical concepts have been used to understand how technical and social systems interact. Dhillon et al. (2021) explained the following about socio-technical concepts: "By socio-technical, we mean how structures (laws and regulations), people (individuals, groups, roles, and organizations), technology (physical technology), and tasks (what data is kept, in what format, who has access) interact." Dhillon et al. (2021) used the different socio-technical concepts to investigate information systems security in organizations further and for example "explore IS security threats and vulnerabilities with a socio-technical perspective to identify advanced risk and vulnerability management strategies" (Dhillon et al., 2021). Tanriverdi & Du (2020), used a similar approach as Dhillon et al. (2021) when investigating corporate strategy changes' effect on IT control in organizations. But Tanriverdi & Du (2020) combined socio-technical concepts of tasks and structures into one category: processes. They use the technology, people, and process triad to research. Where 'technology' refers to the "designing, developing, operating, using, and managing a firm's IT infrastructure" (Tanriverdi & Du, 2020), where they mention firewalls, encryption, and intrusion detection systems as examples. The aim of 'people' is to explain the behavior in an organization by looking at the

employees. The last, 'process,' provides the guidelines and structure that apply in an organization. In the housing association sector, similar social-technical concepts, or the technology, people, and process triad could be used to explain and understand the complex organization of a housing association.

2.1.3 Privacy and information security at Dutch housing associations

The architecture of housing associations in the Netherlands is designed in such a way that they are able to meet the performance goals mentioned by Koopman et al. (2009a) and helps reaches their goal and responsibility, maintaining a high quality of life and providing affordable housing for those in need. Dutch housing associations accommodate, for example, refugees, people with a disability, low-income people, and people above the age of 65. According to M. Naumann, an advisor on housing policy at an Amsterdam-based housing association, it is likely that almost half of the people who rent through their housing association are not skilled in using digital means (Naumann & Van Weersch, 2022). The data of all who are accommodated by housing associations have to be protected because of the impact it could have when placed in the wrong hands. To further illustrate the importance of privacy & information security in the Dutch housing association sector, an example is presented by a news article in Zeeland. Where scammers committed fraud to steal from older people who rent at the housing association called l'escaut (de Jong, 2022b). The scammers identified themselves as police officers and bank employees and, unfortunately, managed to steal money and other valuable stuff. According to the news article written by de Jong (2022b), the scammers had various personal information, such as bank account numbers, date of birth, and other personal data. The housing association l'escaut was also a victim of the TSC hack by the Russian Contri-group at the beginning of march. Where the hackers managed to steal data (phone numbers, addresses, names, and bank account numbers) and released the information on the dark web (de Jong, 2022a). Whether the TSC hack and the leakage of personal data have something to do with each other is not clear (de Jong, 2022b). This case shows the (digital) vulnerability of the people who rent through housing associations and confirms the importance of privacy and information security at Dutch Housing Associations.

For housing associations to best protect their tenant's privacy, the "Baseline Information security Housing Association" (BIC) was launched in 2016. The BIC is a housing association-specific information security standard and aims at improving the availability, integrity, and confidentiality of the information (systems) in the housing association sector (CorpoNet, 2022). The BIC is based on the ISO 27001:2013 and the ISO 27002:2013, both widely accepted as information security standards (Disterer, 2013).

2.2 Cyberthreat Landscape

2.2.1 Introduction to the cyber threat landscape

"As we undergo momentous flows of digital innovations, our lives, and work continue to transform and are evermore characterized by mobility, interconnectivity, virtuality, complexity, hybridity, and fluidity." (Mousavi Baygi et al., 2021, p.423) . This flow of digital innovations influences our modern-day lives and societal changes have become more and more entangled with information technology. These technologies are changing quickly and keep evolving in unpredictable ways; artificial intelligence, data analytics, and robotics are but some of the technological examples that have a far-reaching impact on society (Bailey et al., 2022). Another example of digital transformation is the shift of organizations towards a hybrid way of working and becoming more dependent on the digital systems that enable this change (Leonardi, 2020). According to Faik et al. (2020), technological developments and growing dependency on digital systems can be linked to both positive societal changes on the one hand, as well as complex societal challenges on the other hand.

Together with societal challenges like climate change, migration, and the COVID-19 pandemic, the topic of 'Digital dependencies and Cyber Vulnerabilities' is considered a major global risk, according to the World-Economic-Forum (2022). In their report on Global Risks in the year 2022, the World Economic Forum (WEF) emphasizes the digital risks humanity faces. The WEF concludes that the widespread dependencies of governments, societies, and organizations on increasingly complex digital systems pave the way for cyber threats to grow. "Cyber threats are outpacing societies' ability to effectively prevent and manage them" (World-Economic-Forum, 2022, p.47). Many organizations rely heavily on IT monitoring and management software or use outdated IT systems. These organizations and their IT landscape illustrate the growing digital vulnerabilities and the potential of being victimized by cyber threats. Additionally, the cyber threats themselves increase, becoming more aggressive and extensive (Davis & Mee, 2021).

Atos, a leading global organization in digital transformation, shared its experiences on cyber threats and released a paper about the 'Top 7 cyber threats in the year 2022' (Zakhour & Vasudevan, 2021). Zakhour & Vasudevan (2021) predicted that the following threats would dominate the cyberthreat landscape in 2022: supply chain threats, specialized vertical threats, cloud threats, API threats, external remote services threats, conventional attacks, and the biggest threat of all: ransomware. Zakhour & Vasudevan (2021) also notice the increase in volume, impact, and sophistication of threats, stating that threat actors try to take advantage of new vulnerabilities every year, and organizations must adapt and evolve their cybersecurity every year to protect themselves in this dynamic cyber threat landscape.

Two of those threats, the supply chain threat, and ransomware, can also be found in the attack on the eight housing associations in march this year. The Conti group, who attacked the housing associations, got access to the IT systems of the housing associations through an IT-supplying company called TSC. According to Alzahrani et al. (2022), the Conti group attacks organizations through different phases. They used TSC to access the IT systems of different connected housing associations, utilizing the supply chain threat. Finally, they extorted and misused their gained access via

ransomware, trying to profit from the attack (Monternie, 2022)(Verlaan, 2022).

"The Conti ransomware often leverages phishing campaigns to spread as a starting point of attacks" (Alzahrani et al., 2022, p.13). According to Alzahrani et al. (2022), those phishing emails target victims by sending emails containing Microsoft Office or Google Docs, including links to malicious websites. These malicious websites provide the Conti group with backdoor access to an organization. The component that adds up to the phishing cyber threats is the number of cybersecurity issues that can be traced back to human error, which is around 95% of all the issues (Mee & Brandenburg, 2020). According to Sohrabi Safa et al. (2016), proper information security behavior mitigates the risk of a breach in organizational information security. "Employees' information security awareness plays a vital role in mitigating the risk associated with their behavior in organizations" (Sohrabi Safa et al., 2016, p.71).

2.2.2 Cyberthreat landscape in the Netherlands

The dynamic cyberthreat landscape is noticed by many organisations (Zakhour & Vasudevan, 2021) (World-Economic-Forum, 2022) (Sophos, 2022) (Accenture, 2022) and governments (ministry-of Justice & Security, 2022). Many organizations are evaluating strategies on how to defend themselves against the cyber threats that are all around them. Also, the Dutch Government decided it was time for a national strategy to build a cyber-resilient Dutch society. The Dutch National Coordinator for Counter-terrorism and Security (NCTV), as part of the Dutch Ministry of Justice and Security, introduced the "Dutch Cybersecurity strategy 2022-2028" report in which the NCTV discusses their ambitions and plans on how to create a safer digital society (national Cyber Security Centre Netherlands, 2022). The Dutch strategy focuses on five focal points, being:

1. *Better sight on the cyber threats.*
   The Dutch government wants to invest more people and cyber-resilient IT systems to map the current cyber threat landscape better. They aim to investigate the different cyber threats, the origin of the threat, and whom the threat is aimed at.
2. *More cybersecurity specialist.*
   The Dutch government will take action to get more cybersecurity specialists on the job market.
3. *The government and sectors take responsibility.*
   The government counts on mature and leading organizations in the field of cybersecurity to take responsibility and provide a teaching role in their specific sector. The cybersecurity organization's responsibility will (partly) be placed into the hands of the sectors. Furthermore, new and additional legislation for cybersecurity and the surveillance of this legislation will be drawn up.
4. *Better surveillance, law, and regulations.*
   The Dutch government wants to reorder the responsibility by changing current laws and regulations. Building a resilient cyber system must be a condition on which new systems are designed. New rules will be designed for suppliers of digital products and services.
5. *The information flow from the government towards society must be clear.*

> A new national cyber authority is put into place: The National Cybersecurity Incident Response Team. The dutch national incident response team will help the Dutch society deal with their cyber threats and provide guidance to organizations needing cybersecurity assistance.

The Dutch cybersecurity strategy could also aid the Dutch Housing association sector, as it could look at its own strategy to defend itself against cyber threats and compare it with the Dutch national strategy. In the next section, the process of identifying, assessing, and prioritizing potential threats to an organization is discussed: IT risk management.

2.3 IT Risk Management

2.3.1 Introduction to IT risk management

"A risk is the likelihood of an incident and its consequence for an asset" (Refsdal et al., 2015, p.9). In other words, the risk is considered to be the negative impact that a vulnerability may have on an organization when taking into mind the probability that the vulnerability will be exploited. Many organizations try to face risks in a systematic manner, referred to as Risk Management. In their book on 'Cyber-Risk Management', Refsdal et al. (2015) describe risk management as the coordinated activities to direct and control an organization with regard to risk. In order for risk management to be used efficiently, effectively, and in the right manner, it should fulfill a few demands. The risk management should be based on a risk management framework, which should act in accordance with several risk management principles, both the principles and the framework must be decided upon by the general management of an organization. The management should safeguard the risk management process, as described in Figure 2 (Refsdal et al., 2015). With continuous and finite parts of the process, 'communication and consultation' together with 'monitoring and review' happen in a continuous fashion and the 'risk assessment' is done routinely.

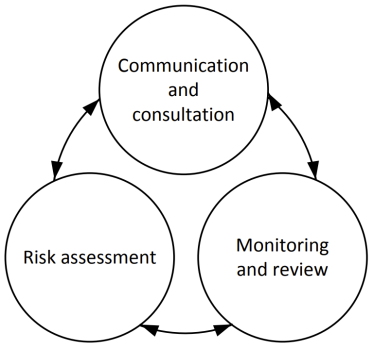

Figure 1
Risk management process. Reprinted from Cyber-Risk Management (p.13), by A. Refsdal, b. Solhaug, & k. Stølen, 2015, retrieved from https://link.springer.com/content/pdf/10.1007/978-3-319-23570-7.pdf : Springer. Copyright 2015 by Springer

In the digital society we live in today all organizations use information technology systems. In order to protect those IT systems from risks, effective IT risk management should be an important part of every organizations security plan (Goguen et al., 2002). In a risk management guide for information technology systems, Goguen et al. (2002) provide a guide for the development of a risk management plan, containing both practical as well as theoretical guidance towards the assessment and mitigation of IT risks. The different steps in the guide are set in order to accomplish three main objectives, the objectives being:

1. Secure IT systems and data. Protect the organizational information when it is stored, being processed or being transferred.

2. Enable management to make informed IT risk management decisions.
3. Enable management to empower the IT systems with the help of supporting documentation based on the risk management performance.

In IT risks management, a few stakeholders should participate in the process in an organization. Management (IT) consultants, IT personnel, and supporting personnel can all play a role in effectively managing risks. Important functions include senior management, the Chief Information Officer (CIO), system owners, Business and functional managers, IT managers, and security officers. According to Goguen et al. (2002), these stakeholders will be involved in a few steps in the risk management process. The first step of the process is the risk assessment, the second step is the mitigation of risks, and the third and last step is making the process ongoing and evolving.

2.3.2 Information & Risks

A part of the Dutch Ministry of Justice and Security, the National Cyber Security Centre (NCSC-NL) focuses on the understanding of the cyber threat landscape, the connecting of parties, knowledge, and information, and the prevention of damage to society through the reduction of threats (national Cyber Security Centre Netherlands, 2022). The NCSC-NL tries to contribute to the Dutch cybersecurity strategy using fundamental, applied, and scientific research. In 2020, the NCSC-NL published a report on Risk Management. They explained how the ownership of information and the associated responsibilities have to be clear to manage the risks (national Cyber Security Centre Netherlands, 2020). The audience the NCSC-NL tries to reach with this report are the boards, management teams, and CISOs (Chief Information Security Officers) of organizations that depend on information to perform their core activities, like housing associations. In the report, at first, the focus is directed on how to *identify and manage information*, as can be seen below (national Cyber Security Centre Netherlands, 2020):

Role of the board

- The board must manage information as an agent of production (like labor and capital) and promote this point of view among the whole organization.
- Hold information owners accountable for their responsibility.

Ownership of information

- Information should have a direct owner.
- Line managers, responsible for the everyday management of the organization, are suitable information owners.
- Information owners should be given support from the information management team to fulfill their tasks.

Information management

- Requires expertise in the topic of information management.
- Provides the support required to manage the information. Do not have control over the information. This control lies with the information owners.
- Information management should have an independent position within the organization.

- Should have direct access to the board and an, by the board approved, information policy.
- Standardize and clarify what is expected of the information owner.

Identifying information
- Coordinate and map the information landscape within the organization. (Include external information sources in the information overview)
- Retain the insights obtained by the information management. Make the holding of the insights part of the change management processes.

Risk-aware behavior
- Create clear instructions on how to work with information.
- Create awareness among all employees, especially around important or sensitive information. Provide training courses and awareness campaigns.

Secondly, the focus is aimed at how to *identify and manage the risks* connected to the information, as can be found below (NCSC-NL, 2020):

Role of the board
- In the end the board is responsible and in case of an information-related incident, will be held accountable.

Ownership of risks
- Information owners should report about the fulfillment of their responsibility to the board. The board should be able to make changes where it is necessary.

Chief Information Security Officer (CISO)
- Has three different roles in the support of the information owners, being:
  Give *advice* on information security.
  Coordinate the information security specific tasks. For example, supervision of risk analyses, plan penetration tests, set up awareness campaigns, record and report incidents, set up and manage the information security management systems (ISMS) as described in ISO 27001.
  Audit on information security.
- CISO should be autonomous and independent with direct links to the board and line management.

Identifying and managing risks
- Identify, evaluate and manage risks through the ISO 31000 and ISO 27005. Use the following steps:
  1. Risk analyses
  2. Selection of measures
  3. Implementation of measures
  4. Monitoring of progress and feedback

2.3.3 IT risk management in frameworks

In this section, three IT risk management frameworks are further explained.

ISO/IEC 27005:2022 The ISO/IEC 27005 is a standard on information security, cybersecurity, and privacy protection and offers guidance on Information Security Risk Management (ISRM) (Agrawal, 2017) (ISO, 2022c). The identification, assessment, and prioritization of risks are part of the ISO/IEC 27005 and should be used as a reoccurring process enabling improvement in both performance and decision-making (Agrawal, 2017). The risk management process as described in the ISO/IEC 27005 can be seen in figure 3 (Motii et al., 2015).

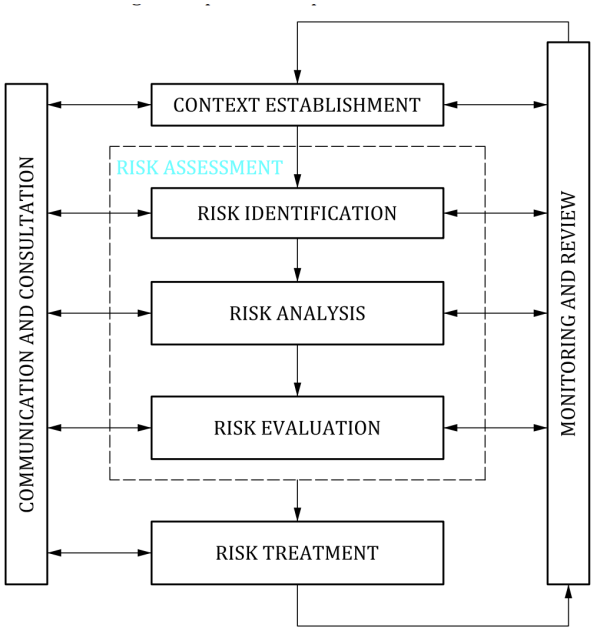

Figure 2
Risk management process. Reprinted from 'Guiding the selection of security patterns based on security requirements and pattern classification', by Motii et al., 2015, retrieved from https://www.researchgate.net/publication/289535525: ACM. Copyright 2011 by ISO/IEC

ISO 31000:2018 ISO 31000 is a standard on risk management and gives guidelines that can be customized to any organization (ISO, 2018). The standard provides principles on effective and efficient risk management, a risk management framework, and the risk management process.

NIST Cybersecurity Framework In their book on 'Cybersecurity Risk Management: Mastering the fundamentals using the NIST Cybersecurity Framework', Brumfield et al. (2021) describe the NIST framework as a framework that is built upon the concepts of risk management. Which is "the ongoing process of identifying, assessing, and responding to risk." (p.19). With the NIST framework, organizations can evaluate whether they want to mitigate, transfer, avoid or accept risks, based on their probable impact on the organizations' critical processes and services. The framework aims to

provide organizations with means to understand, manage, and communicate their cybersecurity actions. The NIST frameworks core (shown in figure 3) is a set of themes, where the goal is to organize cybersecurity actions alongside the different themes. The different themes are 'identify', 'protect', 'detect', 'respond' and 'recover'. At each of these themes, multiple categories of activities are connected. The themes and connected activities can be found in appendix A (figure 11).

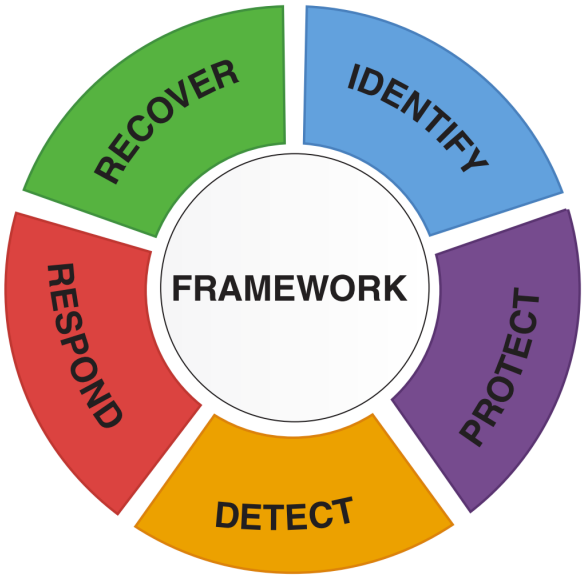

Figure 3
NIST Core Framework. Reprinted from 'Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework', by Brumfield et al., 2021, retrieved from https://ieeexplore.ieee.org/book/9820924: John Wiley & Sons, Inc., . Copyright 2022 by Cynthia Brumfield and Brian Haugli

The NIST framework divides organizations according to "how an organization views cybersecurity risk and the processes in place to manage that risk." (Brumfield et al., 2021, p.21). According to Brumfield et al. (2021) the division is made according to four levels, or tiers, as they are called in the NIST framework. Setting out from Tier 1 (partial) towards Tier 4 (adaptive). A summary, as mentioned by Brumfield et al. (2021) of the different Tiers is given below.:

- Tier 1 (Partial): "Risk is managed in an ad hoc and sometimes reactive manner. There is limited awareness of cybersecurity risk at the organizational level with no organization-wide approach to cybersecurity. The organization may not have the processes in place to participate in coordination or collaboration with other entities." (p.22)
- Tier 2 (Risk Informed): "Management approves risk management practices, but they may not be an organization-wide policy. There is awareness of cybersecurity risk at the organizational level. Still, an organization-wide approach has not been established, and the organization understands the broader ecosystem but has not formalized its participation in it." (p.22)

- Tier 3 (Repeatable): "The organization's risk management practices are approved and formally adopted as policy. There is an organization-wide approach to risk management. The organization collaborates with and receives information from partners in the wider ecosystem." (p.22)
- Tier 4 (Adaptive): "The organization adapts its cybersecurity practices from lessons learned. Cybersecurity risk management uses risk-informed policies, procedures, and processes and is part of the organizational culture and the organization actively shares information with partners." (p.22)

"Risk management framework is one of security assessment tool to reduction of threats and vulnerabilities and mitigates security risks." (Zhang et al., 2010, p.1328) According to Zhang et al. (2010) a risk management framework could be used to better understand critical areas of focus. Furthermore, a framework helps to identify threats and vulnerabilities. The three risk management frameworks presented in this chapter could help the Dutch housing association sector because of the IT risk management tools they offer.

2.4 Privacy & Information Security

2.4.1 An introduction to privacy & information security

In 1890, Brandeis and Warren wrote "The Right to Privacy" in which they stated that "a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sound" . In other words privacy is every one individual right to be let alone, or as Westin (1967) would write it, "to control, edit, manage, and delete information about themselves and decide when, how, and to what extent information is communicated to others". Today, the right to be let alone is still as important but has become more complex, as data privacy has become one of the biggest challenges faced by the (digital) society (Fainmesser et al., 2022).

Privacy and security have the concepts of appropriate use and protection of information in common (Song et al., 2017). The term for information security provided by the National Institute of Standards and Technology (NIST) is as follows: *"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (Kissel, 2013)*. Kissel (2013) further explain information security by using three core principles, also known as the "CIA triad" or "Security Triad" (Pfleeger et al., 2015). The three core principles, as shown in figure 5, are explained below:

- **Availability**
  The guarantee of timely and reliable access and use of information.
- **Integrity**
  Securing information against unauthorized or irregular modification or destruction of information.
- **Confidentiality**
  The preservation of authorized limitation on the access and disclosure of information.

Figure 4
The CIA Triad. Reprinted from 'Implementing an Information Security Management System' (p.8), by Chopra and Chaudhary (2020), retrieved from Tilburg University Library: e-book. Copyright 2020 by Chopra and Chaundhary

However, according to many, the CIA triad is incomplete and other principles could be added to the CIA triad in order to complete it. The five principles that could be added are: accountability, authentication & trustworthiness, auditability, non-repudiation and privacy (Cherdantseva & Hilton, 2013) (Cherdantseva et al., 2016). In this research the CIA triad will be used in addition with the principles 'privacy' and 'auditability' for these two add the most value to the CIA triad in this research. The definitions of the principles being as follows, according to Cherdantseva & Hilton (2013):

- **Privacy**
  "An information system should obey privacy legislation and it should enable individuals to control, where feasible, their personal information (user involvement)" (p.552)
- **Auditability**
  "An ability of an information system to conduct persistent, non bypassable monitoring of all actions performed by humans or machines within the system" (p.552)

In order to guarantee and sustain information security, all sorts of information need to be protected from threat sources of any kind, including cyber threats but the security of information are not only limited to threats that arise from the cyber landscape (Refsdal et al., 2015). In order for organizations to govern their information security, they must realize that information security encloses *technology, processes* and *people* (Veiga & Eloff, 2007). Furthermore, organizations must take a coordinated approach to identify and managing information security en privacy risks because both will benefit from collaboration to reach the shared objective: security (Ross, 2018).

2.4.2 Privacy & information security in frameworks

According to the International Organization for Standardization (ISO), a standard is a formula that explains the best way of doing something (ISO, 2021). A standard that is used in the Dutch Housing Association sector to help guarantee availability, integrity, confidentiality, privacy, and auditability, is called the BIC (Baseline Information Security Housing Associations), as discussed previously in section 2.1.3. The BIC is based on the ISO/IEC 27001:2013 and the ISO/IEC 27002:2013, both those ISO standards have been revised and became the ISO/IEC 27001:2022 and ISO/IEC 27002:2022 (ISO, 2022a) and because these standards are used in the Dutch Housing Association sector they will be further explained in this section.

ISO/IEC 27001:2022 The ISO/IEC 27001 is an international standard designed by the International Organization for Standardization (ISO) together with the International Electrotechnical Commission (IEC). Organizations of all types, sizes, and natures can adapt this standard to establish, implement, maintain and continuously improve their information security management system (ISMS) (ISO, 2022a). The ISMS is put into place to safeguard the confidentiality, integrity, and availability of information with the use of a risk management process. It is important that organizations integrate and scale the ISMS with their organizational needs, processes, and management structure, along with the consideration that information security is the design of the information systems, processes, and controls (ISO, 2022a). According to the ISO (2022), organizations will benefit from the implementation of the ISO/IEC 27001 because it offers information security and increased cyber-resilience on an organization-wide scale. People, technol-

ogy, and processes are all included in the holistic approach of the ISO standard. In the ISO/IEC27001:2022 there are 93 controls divided over four sections:

1. Organizational controls
2. People controls
3. Physical controls
4. Technological controls

ISO/IEC 27002:2022 The ISO/IEC 27002 standard provides a set of recommendations for general information security controls and in addition guidance on how to implement the controls (ISO, 2022b). A control is a *"measure that maintains and/or modifies risk"* (ISO, 2022b). According to the ISO, the standard is designed for all types, sizes, and natures of organizations, that use an ISMS based on the ISO/IEC 27001; who want to implement information security controls based on best practices, and who want to develop organization-specific information security management guidelines (ISO, 2022b). In order for an organization to adopt the standard it must first determine its own information security requirements, according to the ISO/IEC 27001 there are three sources of information security requirements, these sources being: a *organizational risk assessment*, the *legal, regulatory and contractual requirements of an organization* and the last source being a *set of principles, objectives and business requirement* (ISO, 2022b).

2.5 Literature review summary

The Dutch housing association sector plays a vital role in providing the service of affordable housing. Furthermore, the sector provides the service of affordable housing to low-income tenants (Koopman et al., 2009b). However, for the Dutch housing associations to perform this service, they must also protect their tenant's privacy & information. The "Baseline Information security Housing association", also called the BIC, was launched in 2016 to provide the Dutch housing association sector with a baseline for information security. The BIC is a housing association-specific information security baseline, based on the ISO standards (ISO 27001:2013, ISO 27002:2013) (CorpoNet, 2022). To investigate information security further, Dhillon et al. (2021) used the socio-technical concepts of structures, people, technology, and tasks. Also mentioned by Tanriverdi & Du (2020) as a 'people, process, and technology' triad, which could also be used to explain and understand the complex organization of a housing association.

The cyber threat landscape is constantly changing, and new threats are emerging all the time (World-Economic-Forum, 2022). There has been a significant increase in cyber threats on the one hand and growing digital vulnerabilities on the other (Davis & Mee, 2021). These attacks can take many forms, such as phishing, malware, and ransomware, and organizations must adapt and evolve their cybersecurity to protect themselves in this dynamic cyber threat landscape (Zakhour & Vasudevan, 2021). Furthermore, according to Sohrabi Safa et al. (2016), employee awareness of information security plays a vital role in mitigating the risk of a breach in organizational information security. Another factor that plays an important role in mitigating the risk of a privacy & information security breach is IT risk management Goguen et al.

(2002). IT risk management is an essential tool for addressing cyber-attack risks. The risk management process involves the 'risk assessment' phase, which should be done routinely. The 'communication and consultation' phase should happen continuously. The 'monitoring and review' phase should also occur in a continuous order (Refsdal et al., 2015). A risk management framework is a security tool that aims to reduce threats and vulnerabilities and mitigates security risks (Zhang et al., 2010). For example, the NIST cybersecurity framework provides organizations with means to understand, manage, and communicate their cybersecurity actions (Brumfield et al., 2021). Another example is the ISO/IEC 27005 standard, which offers guidance on information security risk management (Agrawal, 2017) (ISO, 2022c). According to Agrawal (2017), the framework should be used in a reoccurring process to enable improvement in performance and decision-making.

Privacy & information security are closely related, and a coordinated approach can be used to achieve the goal of security (Ross, 2018). According to Pfleeger et al. (2015), information security can be explained using the following three terms: Availability, Integrity, and Confidentiality (CIA). However, Cherdantseva & Hilton (2013) suggests principles could be added to the CIA triad to complete it further. Privacy and auditability are both mentioned as principles that would further complete CIA (Cherdantseva & Hilton, 2013) (Cherdantseva et al., 2016). For organizations to help guarantee information security and increase their cyber-resilience, the ISO 27001 and ISO 27002 are standards that provide guidance and control (ISO, 2022a)(ISO, 2022b).

Overall, this literature review explores the different topics that could benefit the Dutch housing association sector by better securing them against cyber vulnerabilities. The literature review suggests that for housing associations to protect the privacy & information in their organization, and thus their tenants, IT risk management could be used to address this issue. Because to protect IT from risks, effective IT risk management should be an important part of every organization's security plan (Goguen et al., 2002).

3 Methodology

This chapter further specifies how this thesis aims to find answers to the research questions and what steps are necessary to find these answers. The first paragraph explains which methods are used in the research and why they are used. Afterward, the research design and the quality of the research design are discussed. In the last two sections of this chapter, the data collection and how this data is analyzed are described.

3.1 Method selection

The methods used in the research are a literature review, case-study research, and semi-structured interviews with experts. The methods are used to help reach this thesis's main goal, which is to answer the main research question: *"How could Dutch housing associations actively use IT risk management to manage their cyber-vulnerabilities?"*. The internal variables, external developments, IT risk management, privacy & information security, and the Dutch housing association sector are investigated throughout the literature review, the case-study research, and the semi-structured interviews.

With the selection of participants for the semi-structured interviews and case studies, the use of non-random criteria like availability, geographical proximity, and expert knowledge of the participant is considered. In other words, the data will be acquired through non-probability sampling. Although non-probability sampling has its limitations, because of the subjective nature when choosing the sample, this sampling method is still beneficial because of the limited amount of resources, time, and workforce available (Etikan et al., 2016).

3.1.1 Literature review

To gain valuable insights, theories, and information, first, a literature review is conducted, which can be found in Chapter 2. The research done by (Levy & J. Ellis, 2006) on a systems approach to conduct an effective literature review in support of information systems research' provides the framework used for the literature data processing. The literature gathering and screening, processing, and writing are the steps taken to introduce and explain the main topics in this research. Furthermore, the literature review lays the foundation for this research to address the gap in the existing literature. Furthermore, the purpose of the literature review is to investigate and review previous research to develop sharper and more insightful questions about the different topics (Yin, 2014).

3.1.2 Case studies

The literature review is evaluated and complemented with the use of case study research. In his book 'Case Study Research: Design and Methods' Yin (2014) listed three conditions on which to decide whether to use a case study. The three conditions are:

1. The research questions should be based on exploratory questions.
2. The research should not require control of behavioral events.
3. The research should focus on contemporary events.

In section 1.3 of this research, the (sub-)questions are formulated and consist of 'What' and 'How' questions and are of an exploratory nature. Furthermore, the research is based on the examination of the contemporary event, with no possible manipulation of relevant behavior. This research meets all three conditions and as a case study has the unique strength to deal with a full variety of literature, artifacts, documentation, and interviews (Yin, 2014), it will be used in this thesis.

In order for the case study to be more compelling in this research, a *multiple-case study* is conducted. The multiple-case study is designed in such a way that each case is carefully selected to get a better understanding of the Dutch Housing Association Sector in terms of 'privacy and information security', 'IT-Risk Management', 'Cyber-security', and 'Cyber threats'. The cases are selected via the convenience sampling method, where Housing Associations are used as cases because of the geographical proximity and willingness to participate in the research. Of the eight organizations that were invited for an interview, five accepted the invitation to participate in the research. The three who declined to participate in the research did so because of a lack of time.

3.1.3 Semi-structured interviews

Next to the case-study research, the data collection will be done via semi-structured interviews held with experts on the topics investigated in this thesis (DiCicco-Bloom & Crabtree, 2006). The interviews will help to address the gap in the literature and provides relevant insights into the environment in which the exploratory research is done. According to research done by Etikan et al. (2016) on the topic of *purposive sampling*, data gathering is crucial in research and contributes to a better understanding of the theoretical framework. In this research, the selected participants will be identified and chosen because of the information they can provide, based on their knowledge or experience on the topics of interest in this research. As it is typically used in qualitative research, information-rich cases for the most actual usage of available resources, are selected (Etikan et al., 2016). Because of this concentration on people who will be able to assist with the relevant research, the purposive sampling method is used. Further criteria used to select participant is discussed in section 3.3.3. Of the five experts that were invited for an interview, all five accepted the invitation to participate in the research.

3.2 Research design

The research design is the logical blueprint of the thesis and consists of three components. These three components are the literature review, case-study research and expert interviews. Together the components form the strategy in this thesis to answer the research questions. The research design is further discussed in this section of the thesis.

3.2.1 Unit of analysis

The research aims at exploring both the current situation and possibilities of IT Risk Management in Dutch Housing Associations. In order to capture this, the unit of analysis is two-sided. The opinion and ideas of experts on the topics of 'privacy and information security', 'IT Risk Management', 'Cyber-security', and 'Cyber-threats' is analyzed. Furthermore, the Dutch Housing Association sector is part of the unit of analyses and the research captures the perspective of different housing associations.

3.2.2 Quality of research design

The research design is expected to represent a logical set of statements and the quality of the research design can also be judged by applying certain logical tests (Yin, 2014). According to Yin (2014) the tests include "trustworthiness, credibility, confirmability, and data dependability". There are four different tests available to test the quality of the research:

- *Construct validity*: the operational measures for the concepts that are being researched are identified and approved. According to Golafshani (2015), who did research on reliability and validity in qualitative research, *"the construct is the initial concept, notion, question or hypothesis that determines which data is to be gathered and how it is to be gathered."*.
- *Internal validity*: the validity of the research itself (Drost, 2011).
- *External validity*: the domain to which the research's findings can be generalized is defined (Yin, 2014).
- *Reliability*; making sure that the operations, for example, data collection, can be replicated with the same outcome. Reliability is the idea that results or observations are replicable or repeatable (Golafshani, 2015).

3.2.3 Data triangulation

"A major threat to the validity of research is its lack of internal validity" (Barnes & Vidgen, 2006, p.770). The internal validity, or credibility, depends on how well the findings in a research match the reality it observes. The triangulation of data helps the research to validate en check the findings. According to Kaplan & Duchon (1988), who did their research on 'combining qualitative and quantitative methods in information systems research', data triangulation helps to create a fuller picture of the phenomenon that is under study. They say:

"Collecting different kinds of data by different methods from different sources provides a wider range of coverage that may result in a fuller picture of the unit under study than would have been achieved otherwise." (p.575)

Their research on 'data triangulation and web quality metric' Barnes & Vidgen (2006) describes different means of triangulation. The 'validity model' refers to the use of different research methods in order to achieve the validation of the results, with the use of triangulation. Furthermore, they explain the 'complementarity model', this model uses triangulation to describe *"A way of getting a broader and more complete picture of a research context."* (p.770). When looking at the validity model, this research did not reach data triangulation in the case studies. Unfortunately, in all the examined cases only one employee participated in the research.

However, a complementarity approach to data triangulation was used to get a broader and more complete picture of the researched context, being the Dutch housing association sector. The literature research, along with the expert interviews were methods used to get a more complete picture and increase internal validity.

3.3 Data collection

This subsection will explain how the data is collected through the use of the different methods in line with the methods presented in section 3.1.

3.3.1 Data from literature review data

The data used for the literature review will be secondary data related to the main concepts or variables, being: *'privacy and information security, 'the Dutch housing Association Sector', 'IT-Risk Management', 'cyber-threats', 'cyber-security'* and *'cyber-security frameworks'*. The secondary data sources that will be used in the literature part of this research will primarily be from Information Management related journals, obtained via the Tilburg University Library. To safeguard the reliability, of the literature review the most used scientific journals will be the MIS Quarterly, Management Science, INFORMS Journal, Information Systems Research, and other journals from within the field of Information Management and related topics. The academic data sources obtained from scientific journals are complemented with relevant sources from the business and public sector, for example with business or governmental reports on the topics or relevant news articles.

3.3.2 Data from case studies

As explained in section 3.1.2 a multiple-case study is used as a source of data. Semi-structured interviews are used to retrieve the data from the cases. Adequate cases are selected via the convenience sampling method, a non-probability sampling method, where the population is the Dutch Housing Association Sector. The cases selected can be found in table 1 and are selected because of their willingness to participate. Among the selected housing associations, there is one who was a victim of the TSC-hack. The criteria that the participating employees from the selected cases have to meet are:

- The participant is an employee in a Dutch Housing Association within the following function or role: (Senior-)manager, IT-, consultant, Chief Information Officer (CIO), security officer, information security officer, privacy officer or another function / role connected to the topics of 'privacy and information security', 'IT-risk management' or 'cyber-security'.

The function (or role) of each case-study participant can be found in table 2 or in appendix C, table 3.

Case number	Dutch Housing Association	Size in rentable units	Number of employees
C-1	Welbions	15.000	127
C-2	Wonen Zuid	14.000	175
C-3	Beveland Wonen	11.000	82
C-4	Alwel	25.000	246
C-5	Stadlander	15.000	183

Table 1
Case selection

3.3.3 Data from semi-structured interviews

Semi-structured interviews are used as a source of data in both the case-study research and the expert-interviews. The people participating in the research must meet certain criteria to be selected as participants in the study. Participants are selected via the purposive sampling method and thus are selected based on their study purpose with the presumption that each individual participant will provide valuable insights and useful information to the research. In addition, with purposive sampling, the sample size is determined by data saturation and not via a statistical power analysis (Etikan et al., 2016). According to Saunders et al. (2017) saturation has achieved acceptance as a methodological principle in qualitative research, it indicates whether or not further data collection is necessary based on the data collection so far. In their research on 'Saturation in qualitative research', Saunders et al. (2017) propose 4 different models to achieve saturation in the research process. Because of the conventional nonspecialist approach in this study, the *inductive thematic saturation* model is used to know where the point of data saturation is reached. The inductive thematic saturation model relates to the emergence of new codes or themes during the analysis stage in the research (Saunders et al., 2017).

The criteria that participants have to meet in order to get selected are as follows:

- The participant is an expert in the field of 'privacy and information security', 'IT-risk management' or 'cyber-security' and is familiar with the Dutch Housing Association Sector.

All the selected participants were available and willing to participate in the research. An overview of the participants can be found in table 2. A comprehensive overview can be found in Appendix C, Table 3.

Number	Function / Roles
E-1	Partner / IT Auditor / Forensic Investigator
E-2	Business Consultant / IT security & privacy specialist
E-3	Partner / IT security & privacy specialist
E-4	Victim of a Cyber-hack and speaker on cyber-security conferences
E-5	Director / Security Officer
C-1	Business Controller / Risk Management specialist
C-2	Information Manager
C-3	Information Policy Advisor / Security Officer
C-4	Business Controller
C-5	Information Manager / Security Officer

Table 2
Semi-structured interviews & Cases: Participants, Function / Roles

3.3.4 Interviews

Semi-structured interviews are used for the collection of data in both the case-study research as in the expert interviews. The interview guide was designed with the aim

of creating a data collection tool by operationalizing abstract concepts en theoretical knowledge into a logical and coherent form, as described by Kallio et al. (2016) in their paper on '*Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide*'. In other words, the interview guide is based on chapter 2, and questions on the main topics are prepared. During the interviews, different kinds of spontaneous follow-up questions can be asked in order to clarify the answers given, gain additional information, or for the fluency of the interview (Kallio et al., 2016). In some interviews, questions are skipped because the topic had already been discussed and the information provided. All interviews were held on a one-on-one basis between the 29th of November and the 14th of December in 2022. The duration of the conducted interviews is between 43 minutes and 1 hour & 25 minutes.

All the participants were informed on the topic and purpose of the research and interview in advance through an information letter that had been sent, via e-mail, prior to the interviews. The information letter can be found in appendix F. All the interviews were conducted via Microsoft Teams. At the beginning of the interview, explicit permission was asked and each participant gave their permission to record, transcribe, translate and use the interview in the research. The interviews were recorded en automatically transcribed by Microsoft Teams, later the automatic transcription was corrected by hand. The interviews were all held in Dutch because the native language of all the participants is Dutch. The first version of the transcripts is in Dutch and this version of the transcript was shared with the participant. This allowed the participant to give feedback on the transcript. Five participants gave feedback on the transcripts, requesting changes to the transcript. The changes asked were either spelling revisions or improvements to the textual structure of the transcript. In one case, some extra clarification to the answers given was provided. All changes asked the to transcripts were corrected. The Dutch version of the transcripts is translated into English, with the use of the translation software called DeepL. The automatic translation was later corrected by hand, the English version of the transcripts can be found in appendix H (Case-study interviews) and in appendix I (Expert-interviews).

3.4 Data analysis

The data analysis is carried out by systematically following four steps to get a basis for building the data analysis structure used in this research. The data analysis structure not only provides visual aid, but it also provides a graphic representation of how raw data is processed to terms and topics during the analysis phase (Gioia et al., 2012). Throughout the data analysis phase, the data analysis software ATLAS.ti web version was used to code the interview transcript. ATLAS.ti was used because *"By using ATLAS.ti, it becomes much easier to analyze data systematically and to ask questions that you otherwise would not ask because the manual tasks involved would be too time-consuming.* (Friese, 2012, p.1). However, because of the small number of interviews, the coding itself was done by hand. The only data coder involved in the process was the author of this thesis.

Step 1. In the first phase of coding, the open coding phase, the interview transcripts were carefully read and categorized into codes based on the information given by the participants. In this stage, many different codes were used and eventually brought back to a more manageable number, creating the first-order codes. (Gioia et al., 2012). All

first-order codes were derived from the data. However, some first-order code names were identified based on the literature review.

Step 2. In the second phase of axial coding, the interview transcripts were reread, and the first-order codes were evaluated, trying to answer the important question of "What's going on here theoretically?" (Gioia et al., 2012, p.20). In this stage, the interview data is connected to the literature to acquire additional analytical insights (O'Neil et al., 2022). Second-order themes are created by combining the literature with the data from the interviews. All second-order theme names are identified based on the literature review. For example, the '*Organisation*', '*Governance and policies*' and '*IT landscape*' codes were combined to the second-order theme of *'Processes'*.

Step 3. In the third phase of selective coding, the second-order codes are distilled into aggregated dimensions. At this stage, special attention should be given to creating main themes that are useful for answering the main and sub-research questions (O'Neil et al., 2022). The aggregated dimensions used in the data analysis structure are '*Internal variables*', '*External variables*', '*IT risk management*' and '*Privacy & information security*'.

Step 4. In the fourth and final phase, the first-order codes, second-order codes, and aggregated dimensions are processed into a visual representation of the data analysis structure, which can be found in figure 5.

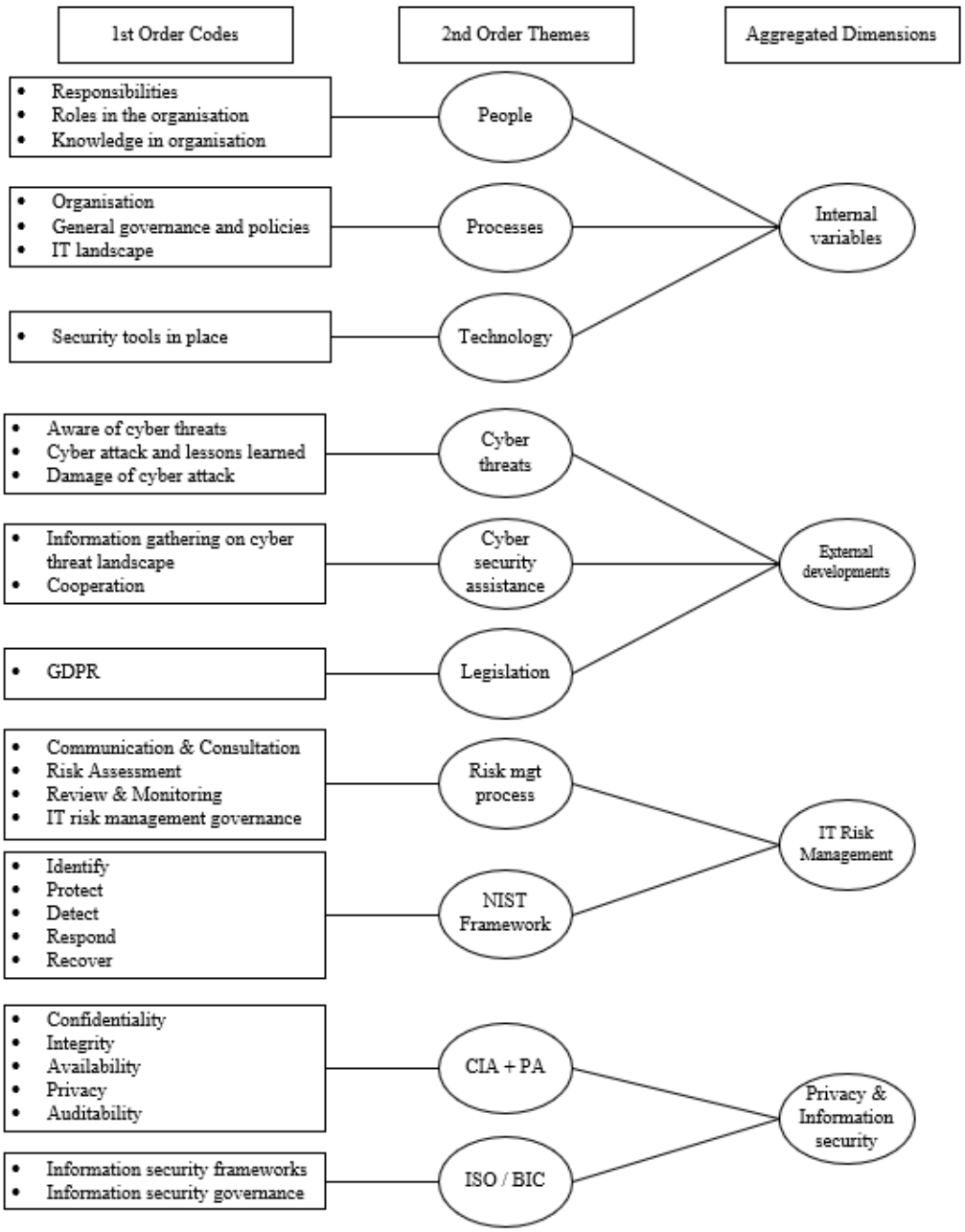

Figure 5
Data analysis structure

4 Results

In this chapter of the research, the results obtained from the qualitative data analysis are presented.

4.1 Internal variables

The aggregated dimension '*Internal variables*' is the combination of the second-order themes of '*People*', '*Processes*' and '*Technology*', as shown in figure 6. The *internal variables* are important variables that show how a housing association organizes itself.

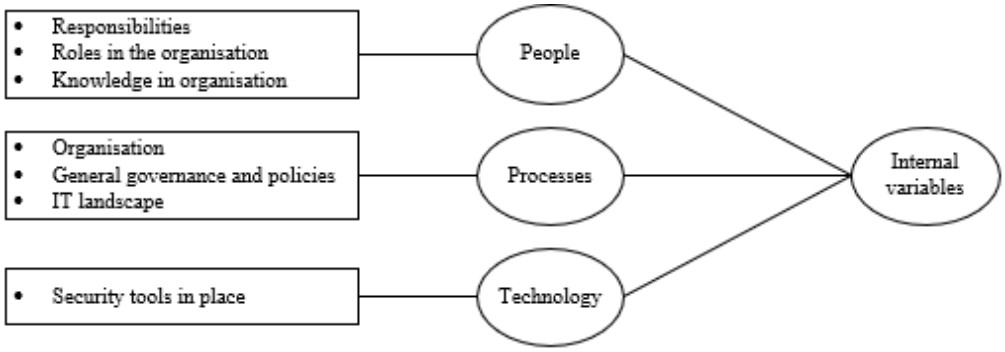

Figure 6
Internal variables in housing associations

4.1.1 People

The second-order theme of *People*, is the combination of responsibilities, roles, and knowledge in organizations. These were all first-order codes that were mentioned many times during the different case studies and expert interviews, making the second-order theme of People a well-discussed theme when talking about internal variables in Housing Associations.

The responsibilities of different roles in the organizations are mentioned in all the case studies and expert interviews. The board of a housing association has the ultimate responsibility of managing the cyber-security, as underlined in all the interviews. *"That [Cyber security] is ultimately the executive board's ultimate responsibility, and he or she will formally be responsible"* is stated by expert-2. *"But, I think it's much more important that responsibility be taken. It starts at that [executive board] level, and then of course some responsibilities just have to be delegated to other management team members."* expert 2 continuous. Also, the interviewee of case-4, working at Alwel (case-4), indicates that the board has ultimate responsibility, but delegates this responsibility to the rest of the organization and managers. *"the board is always responsible but I think the responsibility lies primarily with the operations manager, who in turn has an I&A team manager to make sure cyber security is in place. This means that the information security policy we have in place as a housing association, although the responsibility for this is delegated to the organization and the manager of operations, the board is ultimately responsible"*. And this is the case at Wonen Zuid (case-2) where the responsibility is *"delegated from the board to me as manager I&A*, says the interviewee of case-2. At Beveland Wonen (case-3), the interviewee of case-3 mentioned that the responsibility of handling the cyber security is vested in him as a security officer, but that he is not ultimately responsible. Also at Welbions (case-1) and Stadlander (case-5), the ultimate responsibility lies at the executive boards.

All participants underline the ultimate responsibility of the board, however, some highlight the role of the entire organization when it comes to the responsibility of cyber security. Expert-1 noted that *"Everyone in an organization, from high to low, left to right, should feel responsible"*, the interviewee of case-1 stresses the importance of cyber-security and the shared responsibility *"Cybersecurity is very important in this world. Although management is ultimately responsible for addressing cybersecurity, everyone must feel responsible for it and be aware of its importance."* Also on the part of IT risk management, the board is mentioned to be responsible *"Yes, organization-wide, this is the case in every organization. Awareness of this [risk management] should be present at all levels, especially at the board level"* Expert-5 stated, but he adds *"The IT component is becoming increasingly important for housing associations, especially for the administrative side of housing"*. Expert-1 says the following about the responsibility for managing IT risk: *"It is not an IT party, but a matter that has to be looked at from the business perspective. It is also important to get feedback from different multidisciplinary teams and employees. The risk profile and risk appetite will often be determined by management or the board"*.

About the responsibility of IT risk management, Expert-2 declared the following: *"it [IT risk management] is something for the whole organization en must be addressed from the top down. The responsibility lies at the management team level, with a board of directors closely involved"*. Within the housing association Welbions, the I&A and Control department is responsible for different parts of IT risk management. Where I&A looks at the technology part, Control is responsible for the strategic side, such as reporting about information security risks, as the interviewee of case-1 mentioned. Wonen Zuid and Alwel have the same structure, with the Control department which gives advise on risk management, the I&A department which is responsible for the mitigation of the risks and the board determines the risk appetite and policy on IT risk management. At Stadlander, the interviewee of case-5 mentions that the responsibility for IT risk management is his, as manager of ICT.

Furthermore, the responsibility of safeguarding privacy in the housing associations is placed in the hands of a privacy officer, in all five cases. The information security aspect is placed in the hands of a security officer, *"We have a privacy officer for that [privacy], he is responsible for that [privacy]. The piece of information security is placed in my hands"* the interviewee of case-3 remarked. The interviewee of case-5 recognizes that the different roles and responsibilities in an organization aren't always clear, *"we need to formulate the roles and responsibilities In the policy more sharply. Nobody knows what they are responsible for in that area, so get a little more specific what roles or and who is responsible for what and include that in the policy documents".* Also Expert-3 doubts if the roles and responsibilities are always clear at housing associations *"I doubt that the roles at corporations are at all well defined in terms of privacy and security policies"*. According to Expert-3, privacy & information security needs to be the responsibility of the whole organization, but it is the responsibility of the board to make sure there is a clear and up-to-date information security and privacy policy.

At Wonen Zuid, the roles of Security officer and Privacy officer are assigned to two separate people *"Because they are two different things"* according to the interviewee of case-2. At Welbions, the organization hired an external Security officer. The interviewee of case-1 mentioned that with smaller housing associations with fewer employees, certain roles can be externally sourced. *we, like other housing associations, do not have internal expertise for a privacy officer or security officer, so we have since had these functions*

performed by an external provider" she says. The hiring of interim or external employees to do a specific job is also noticed by other participants. Expert-5 however addresses the complexity of the matter, *"Housing associations need the guidance to properly safeguard these functions in their own organizations but it is killing if the knowledge remains with the external consultants"*.

The knowledge and awareness of cyber threats and security on all levels of organizations is noted as an important topic in multiple interviews. *"In the end, the most important firewall is just sitting between the monitor and that chair"* The interviewee of case-3 expresses, advancing with *"There was an incident two weeks back I believe at Woongoed in Middelburg. Through the watchfulness of an employee, they were able to limit the damage there. [...] Creating awareness is extremely important in the organization in order to be able to combat it"*. Expert-4 adds to the point of awareness: *"I find it strange that the housing association does have a display near the coffee machine with instructions in case of fire, when the probability of a fire being started is only 1 in 8,000 and the average damage is € 14,000, while there is no cyber plan hanging for the case of cyber incidents, where the probability is 1 in 5 and the average damage is €340,000*". The awareness of employees in the area of cyber threats and security, is an area of interest, mentioned in both case study interviews, as in expert interviews.

4.1.2 Processes

The processes are a second-order theme, comprised of the difference in organizations, the general governance and policies, and the IT landscape. All these first-order codes were mentioned in the interviews when talking about housing associations in general. Housing associations not only differ in size and structure, but also in the way they govern their organization, and organize their IT landscape. The interviewee of case-1 also mentioned the difference between housing associations when it comes to digitization and the dependency on IT: *"The scale of a housing corporation determines how dependent they are on their IT system. Smaller housing associations often have a basic system, and are financially constrained and do not always have the people with the right specialization to digitize their entire system. If there are many older people working at a housing association, this can also affect its reliance on digitization. However, this is not true for all housing associations."*

In all the interviews, the dependency of housing associations on their IT got underlined. The interviewee of case 5 says the following about Stadlander and its dependency on IT: *"When I look at what we have digitized and organized it is no longer possible to work in any other way and keep the business continuity intact."*. A similar answer was given in the case interviews of Alwel, Wonen Zuid, Beveland Wonen, and the expert interviews. When asked about the dependency on IT in the housing association sector, Expert-3 answered the following *"The physical and digital worlds have become increasingly intertwined. [...] So the digitization of housing associations is rapidly increasing and has really taken off."* In different interviews, it is noticed that many important business processes, tools, and applications in housing associations rely on IT and that the IT landscape in housing associations, is one where IT is often outsourced.

Expert-2 mentioned: *"Actually almost every corporation has largely outsourced it [IT]. When it concerns the office IT and actually the whole network, that is often managed by a service provider, an ICT service provider.* Expert-5 also links the use of outsourcing to the size and expertise in organizations, *"although it can still be difficult to handle the complexity of the application and functional management within one's own organization. This is especially the*

case for smaller corporations with 50 to 100 employees, which often struggle to keep expertise on board. As a result, much of the IT and applications are outsourced, with corporation employees often working at the user level." According to the interviewee of case-3, many housing associations did not only outsource their ICT but also their knowledge about ICT. Both the interviewee of case-2 and case-3 underline the importance of staying in control of the outsourced IT, at Wonen Zuid *"We have always run our own data center services through 2019, but from 2020 we have outsourced the entire technical management and the entire technical dispatch, while we have taken a heavy directorial role with respect to our supplier, in the Cyber area."*

The interviewee of case-1 mentioned the importance of good communication with IT providers, *"it is also important that we have good communication with our providers, such as our grid operator, where we have our servers managed."* In multiple interviews, the importance of keeping responsible for IT although it is outsourced, is mentioned. Expert-2 says *"Because outsourcing your IT does not mean outsourcing your responsibilities over IT and thus your data. [...] You have to stay in control and that is precisely where the risk lies."* Expert-3 expresses a similar viewpoint, also mentioning the importance of keeping the responsibility to oversee the outsourced parts of the IT landscape. Expert-1 adds on the matter: *"It is also advisable to review provider agreements carefully to determine where responsibility lies when there is a lot of outsourcing. We have found that there is often overlap in expectations of responsibilities, leading to gaps where no one does anything. It is therefore important to also think about and practice disaster scenarios so that we are prepared when they occur."*

4.1.3 Technology

The second-order theme of Technology is often discussed during the interviews on the base of security tools in place in an organization. Where several security tools that housing associations use, or could use are named. For example, security protocols such as Transport Layer Security (TLS), or tools such as firewalls and antivirus software are mentioned by the interviewee of case-2. Multi-Factor Authentication (MFA), IP restrictions, and conditional access tooling is mentioned by the interviewee of case-5, he says *"there really is a good shell around it"* when talking about getting access to Stadlanders network. The interviewee of case-3 noticed that *"you are never secure enough [...] I do see a few technical measures we can still take."* Expert-1 also mentioned that organizations who apply password policies and use MFA, do not always apply it the right way, *"Overall, I think there is still much to be gained in the Netherlands in terms of cyber security. Some organizations are better prepared than others."*

4.2 External developments

The aggregated dimension '*External developments*' is the combination of the second-order themes of '*Cyber threats*', '*Cyber security assistance*' and '*Legislation*', as shown in figure 7.

4.2.1 Cyber threats

The second-order theme of cyber threats is about the external developments that happen around the housing association sector and influences the sector. The theme arises from the mixture of the first-order codes: Awareness of cyber threats, cyber-attacks and lessons learned and the damage a cyber-attack could do to an organization.

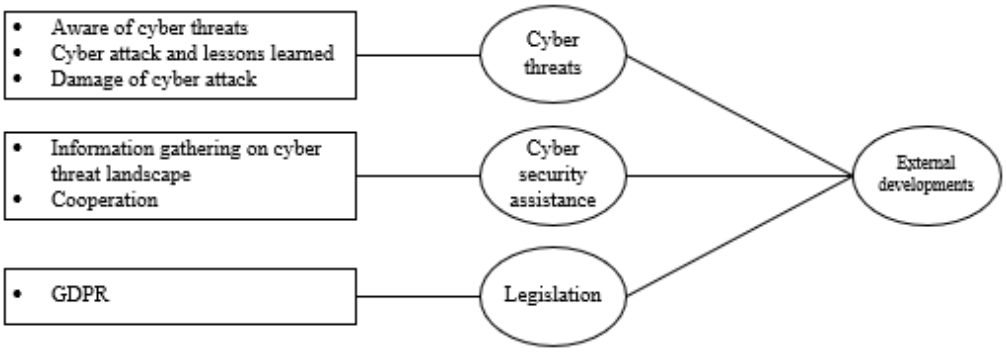

Figure 7
External developments for housing associations

In all the case-study interviews, the participants noted that there is a real cyber threat to their organization and the sector in general. On the matter, the interviewee of case-1 says: *"Lately, we have heard many rumors of cyber attacks involving ransomware. It remains a threat that we must be alert of. Every housing association must realize that they are vulnerable as well."*, also the interviewee of case-3 noticed the threat and mentions *"That threat is very real because we see among our colleagues that they have already become victims in larger or smaller dimensions. And we also notice very frequently that attempts are made by means of phishing, for example."*. The interviewee of case-2 says that the attacks happen on a daily basis, varying in size and danger. *"It is important to always be on guard and take measures to protect ourselves from these threats."* All the participants of the expert interviews underline that cyber threats are real and it is important to be aware.

In the interviews the happening of cyber attacks has been discussed, attacks through different ways and of different sizes. Although Wonen Zuid has not been victimized by a cyber attack, they do have been under siege, says the interviewee of case-2. *"just recently we experienced a severe attack where we had to use extra surveillance for several weeks to protect ourselves. This cost us hundreds of extra hours, but fortunately, we managed to remain undamaged."* Other kinds of attacks that were mentioned in interviews are phishing, business email compromises, ransomware attacks, expert-2 discloses on the matter: *"There are of course at corporations every day numerous attacks that are repelled from phishing to intrusion attempts, or exploiting vulnerabilities et cetera"*. The interviewee of case-4 says that unfortunately, there had been a successful cyber attack on his organization, through phishing and ransomware. The interviewee mentions the following when asked about the lessons learned: *"We want to use these lessons learned and share this knowledge with others in the sector so that they can also move quickly in similar situations. We are creating a separate write-up for this, other corporations are also interested in how we handled this."* Expert-4 underlines the importance of sharing knowledge and experiences, saying: *"There are a number of things to consider when it comes to security against hackers. For example, it is important to share experiences and create lists of points of interest and potential concerns and vulnerabilities, and the solutions to them."*

When talking about the damage a cyber attack can do to an organization, different topics were mentioned. Varying from financial damage, the impact on the IT landscape, processes, business continuity, damage to the organization's reputation, and the loss of

data. Expert-4 stresses the importance of realizing that the damage is not only financial but *"we must also look at what the hack is doing to you and your people. It can lead to burnouts, stress, work disability, rising healthcare costs and work absences, which can be much more costly in the long run than the financial damage."*. Other participants also noted the impact a cyber attack can potentially have on the organisation, its employees and other persons involved.

4.2.2 Cyber security assistance

The second-order theme of cyber security assistance is made up of two first-order codes, the 'information gathering on cyber threat landscape' and the 'cooperation'. When discussed in the interviews, several participants noticed the assistance the housing association gets, and could further receive from external organizations in the area of cyber security. Several ideas, topics, and opinions were given on the second-order theme and were mainly divided into two different codes, one side talking about the information housing associations and the entire housing associations sector could gather in the sphere of cyber threats. The other side of codes was the cooperation with external companies, partners, or with other organizations. In addition, the cooperation between housing associations is analyzed.

Cooperation between housing associations is a well-discussed topic during the interviews. Aiming at different kinds of cooperation, for example, the cooperation between different housing associations. Expert-1 explains the similarities between housing associations and why they could easily cooperate: *"their tenants, used systems and applications are almost the same, but they have different properties with different residents. So yes, they could easily cooperate. They [housing associations] are organizations that are almost completely similar to each other."* Expert-2 underlines the opinion that housing associations could cooperate: *"I think precisely in nonprofit sectors where you have no competition and can actually learn from each other for free and team up with one another."* and observed the regional initiatives to cooperate. *"Can really be much more if you ask me. I do see associations that are looking for each other. [...] Cooperating housing associations in certain regions, for example, Zeeland, is such a region where there is a lot of cooperation on this theme [Cyber security] in order to work together, but also to acquire knowledge together."* In the interview with Expert-4, the regional cooperating initiatives are perceived as well. Mentioning the role of the national network organization of housing associations, Aedes, and another organization, Corponet: *"In the area of security, we are also seeing more and more initiatives for regional cooperation, including by parties such as Corponet and Aedes."* Several other participants, both in case study interviews and in expert interviews note the opportunities cooperating offers. About cooperation between housing associations, the interviewee of case-1 says the following: *"My opinion is that cooperation between housing associations is not sufficiently exploited because too much emphasis is placed on the idea of "my territory" and "my tenants." This is unfortunate because we can learn a lot from each other and save money in the process. There are definitely opportunities to act together when there are problems."*

In the interview with expert-4, the importance of working together was further underlined: *"As for housing associations, I think it's important to have their IT departments collaborate in weekly meetings. That way they can identify threats and share information about current problems. If they do that, they can hire a cyber specialist to help with the solution and share that knowledge again. That's how action should be taken. We need to talk to each other*

and work together to achieve spectacular improvements, but everyone seems so stuck in their own tunnel that they are not doing that". The sharing of knowledge between housing associations is a topic where the interviewee of case-2 says the following about: *"Sharing knowledge about information security is becoming increasingly important. We are affiliated with the special interest group cyber security at Corponet. Where housing associations share information with each other to keep each other informed about threats."* When asked about what could be improved on the area of cyber resilience the interviewee of case 2 adds *"It is important to always remain vigilant and keep working to improve information security. It is also important to keep learning and stay on top of the latest developments and threats in the world of cyber security. It is also good to collaborate with other organizations and share what you know and learn so that everyone can benefit from shared knowledge and experience".*

Furthermore, in all the cases, the intention to cooperate with external organizations on the topic of information gathering about the cyber threat landscape came forward. In some case studies the organization is already cooperating in this area, for example Wonen Zuid, the interviewee of case-2 explained *"We keep ourselves aware of threats in the sector by checking the websites of renowned parties, such as McAfee and Checkpoint. We also follow websites of DTC (digital trust center), NCSC to keep aware of what is happening in the world."* and adds that by joining efforts with a colleague he is organizing the development of a housing association sector specific ISAC (Information Sharing and Analysis Center). The interviewee of case-3 also talks about the sector specific ISAC, together with Corponet. The ISAC will have the goal *"to start providing information security information to the entire housing association sector."*

In the interviews with the interviewees of case-1, case-2, case-3, case-4 & case-5 the cooperation with or the assistance of one or multiple external organisations is discussed. On the one hand, to gather information on the cyber threat landscape. Organisations like Corponet, the DTC (Digital Trust Center) and the NCSC (National Coordinator for Counter-terrorism and Security) are mentioned by the interviewees of case-2, case-3 & case-5, but also in several expert interviews. Expert-3 places a critical note, when asked about housing associations being aware of the cyber threat landscape: *"I notice that few associations actively explore how the [cyber] threat is developing and what this means for the risk analysis you do as an organization and the measures that need to be taken. Some associations have outsourced this to specialized parties, while others do subscribe to online forums or communities to stay informed. The majority, however, seem to have no idea or at least have not actively paid attention to this. How this threat is developing in terms of direction or speed."* Adding that there is need of a quarterly cycle, where the information about the current cyber threat landscape needs to be discussed and tells *"This can hardly be done individually by an association and therefore it is necessary to seek help from parties who can do this on behalf of or with the association."*, stressing the importance of cooperating once more.

On the other hand, the support of external organizations is sought because *"they need the support because the knowledge is frequently not available. [...] We talk about the strategic, tactical, and operational levels and all these levels need to be fed with the right information"* Expert-1 explains. A subject talked about in all case study interviews, with housing associations working together with external parties who help them with their cyber security on all different levels. The interviewee of case-3 mentions the assistance of an external partner to create an awareness program, or do a business impact analysis. The interviewee of case-5 discusses different kinds of risk assessments with the help of an

external organization. The interviewee of case-5 also talks about retrieving knowledge and information from external parties in order for Stadlander to create an incident response plan. In the interview with the interviewee of case-2, he speaks about the partnership with an external organization to get consultation on the technical aspects of information security.

4.2.3 Legislation

Another external development discussed in the interviews was the second-order theme of legislation. Often the link between privacy and the GDPR (General Data Protection Regulation) is made in the case study and expert interviews. The GDPR itself is mentioned in all the interviews, being noted as legislation that every organization has to live up to. The interviewee of case-4 says the following about the GDPR and Alwel: *"The General Data Protection Regulation (GDPR) is an important topic for us to consider. There are different levels we can strive for to comply with the GDPR, the minimum we have to do is of course mandatory. But we also have the ambition to reach a higher level than what we have reached now."* In different case study interviews, the introduction of the GDPR in 2018 was noticed as a reason for housing associations to appoint privacy officers. According to the interviewee of case-2: *"The GDPR (General Data Protection Regulation) went into effect on May 25, 2018. Within Wonen Zuid at that time, there was no specific place or structure where this was properly invested. [...] Only after the Data Protection Act transitioned to the GDPR has this function gained a real position in our organization."*the interviewee of case-5 mentioned something similar when discussing the influence the GDPR had on Stadlander. Parallel to the interviews of case-5 & case-2, in the interview of case-1 the following is said about the GDPR: *"Privacy and information security are high on our list of priorities. To this end, I am a member of the information security and privacy steering committee, a kind of expert group. This is mainly because of the GDPR of 2018. We have been looking for a structure that can help us ensure privacy and information security. We decided to form an expert group with representatives from HRM, I&A or ICT, communications, processes, and myself [Business Controller]."*

In the expert interviews the topic of the GDPR was also discussed, *"Moreover, the GDPR, or the General Data Protection Regulation, is also simply a privacy law that everyone must comply with."* is said in the interview with expert-3. Expert-3 continuous with *"The framework of the GDPR cannot be avoided. This is a hygiene factor on one hand, but on the other hand, there are housing associations that also see it as a way to be trustworthy and do good business, not just because it is required by law. They also see it as their responsibility to make sure everything is in place for employees and other stakeholders with whom they share information and data."* Expert-1 addresses the GDPR in a different way, he explains the following: *"I struggle with the GDPR, good that attention is being paid to the matter but I don't read a word "privacy" in GDPR. But what I actually think is important is information security. There are privacy-like issues in that as well. This is not just important to meet government compliance requirements, that's not the point, you want your information security to be in good condition."* Also expert-2 talks about how housing associations coop with the underlying thought of the GDPR: *"yes GDPR is a legal obligation and we put a checkmark and we comply again. But that is actually the underlying thought of okay, how are we going to make sure that we embed it in all the processes and put the right action there? That that that still mostly falls short, but we do see more and more improvements there as well."* Showing that, according to some experts, housing associations must of course comply with the legislation but may also think about the underlying idea behind the General Data Protection Regulation.

4.3 IT risk management

The aggregated dimension '*IT risk management*' is the combination of the second-order themes of '*Risk management process*' and '*NIST framework*', as shown in figure 8.

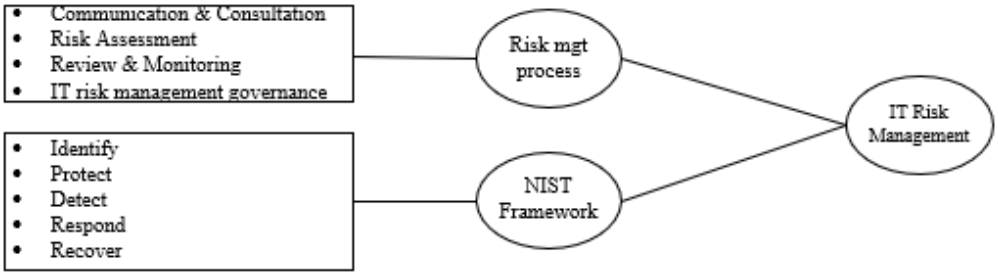

Figure 8
IT risk management in housing associations

4.3.1 Risk management process

The process of managing IT risk is analyzed in multiple case-study and expert interviews. The second-order theme is a collection of the first-order codes about the different stages in the IT risk management process. The 'communication & consultation', 'risk assessment', 'review & monitoring', and the IT risk management governance, could be divided into the IT risk management context establishment and treatment of perceived risks.

According to expert-3 a hack of multiple housing associations in the beginning of 2022 created a sector-wide impulse on several levels of the IT risk management process: *"The eight-fold hack last late March has caused many organizations [housing associations] to focus on creating incident response plans and doing business impact analysis to determine what risks they face, risk assessments are also being done. They are also keeping an eye on the situation to see how they are doing, fewer organizations are watching what is happening in the market. The goal is to identify the impact on the processes, systems, and data when they are hit. It has had an impulse because of the hack."* Different housing associations that are part of the case study talk about risk assessments, mostly about risk identification or risk analysis. The interviewee of case-5 talks about the identification of risks in their organization, with the help of external partners, *"We are now in the process of conducting a Business Impact Analysis (BIA) with Audittrail [external partner] and with NorthWave [external partner] we are doing a complete risk inventory to establish a baseline."* Also at Welbions they are currently doing a business impact analysis: *"It starts with the business impact analysis, where we look at every process. With the question, what exactly are our critical processes? I don't know if many housing associations already have this type of plan, but in our case, we do not have it yet."* says the interviewee of case-1. At Beveland Wonen, they just created a new information security policy in collaboration with an external partner. The interviewee of case-3 declares: *"the result is a risk management policy and risk categorization of assets. This is going to be formally approved soon and then there will be an annual cycle over and over again where these matters will be reviewed."*

So in different case-study interviews, the participants confirmed that their organization is currently working on its IT risk management. At Wonen Zuid they

audit and use penetration tests on a regular basis, according to the interviewee of case-2 they pass the test: *'"When we first had a penetration test performed, a number of things were flagged. We fixed those. We also regularly retest to make sure we keep a clean sheet."*. In the expert-interviews the importance of doing a risk assessment is underlined. However, in all the expert-interviews the monitoring and reviewing part of IT risk assessments and IT risk management as a whole is being advocated. Expert-1 illustrates by giving an example: *"We did an assessment a year ago for a housing association in the neighborhood and it was supposed to return annually. However, a number of people left who were involved in doing this, so it subsided. It is a shame that they are dependent on people here and more should be done to take it all the way up and keep it involved on a yearly basis. It is important for organizations to look in the mirror on a regular basis."* In the interviews with expert-2 and expert-3 similarities can be found when talking about the frequency of doing a risk analysis. Expert-3 says on the matter: *"Risk analysis is very important to do at the beginning because it is an almost unexplored area. [...] It may not even be in its early stages. So it is important to address this quickly and determine what we have to secure, how to secure it, and at what cost."* When asked about the frequency of which IT risks should be evaluated, expert-4 announces the following: *"Things are moving very fast in the cyber world. I would say start with two weekly consultations. Further, have a penetration test done twice a year or maybe four times a year. Or alternatively, instead of a pen test, invite an ethical hacker to conduct attacks to see if you have things in the right order internally as an organization."* Expert-5 also stresses the importance of doing regular assessments, naming the Data Privacy Impact Assessment (DPIA) as a tool to use to check what data organizations handles.

Both expert-4 and expert-5 argue for the creation of user groups with regular meetings to discuss IT risk. Expert-5 mentions: *" So both information sharing and discussion. We have taken measures to mitigate the risks, but are they still effective? It would be nice if we could meet with a mix of people, such as technical and legal experts, with some regularity. For example, every six weeks."* and expert-5 says: *"Consultation with IT guys, guest speakers, ethical hackers, cyber specialists and I imagine quarterly evaluation so 4 times a year."* On the topic of monitoring & reviewing the IT risks, the interviewee of case-1 says the following: *"I think continuous monitoring is important because otherwise risk awareness is lost if you just put check marks and make reports. Active monitoring is also important, because it's not just about making reports, but doing something in response to the risks we see."* A management method for the monitoring and reviewing of IT risk that is mentioned in a few interviews is the Plan Do Check Act process (PDCA). It is mentioned in the interviews of case-2, expert-2, and expert-5 as a method that could help with IT risk management. About the PCDA process, expert-5 noted the following: *"By assessing the effectiveness of the measures and repeating this process regularly, the plan-do-check-act cycle is well established. I think this can be complex at times, especially if it's not in your DNA."*

On the topic of IT risk management governance and the IT risk management policies in housing associations Expert-1 says the following *"If it's [an IT risk management policy] there at all, it's often the latter [Not frequently updated]. It is important to regularly revise how you organize your tasks and whether you are doing enough to keep your household running smoothly. It is advisable to do this at least once a year, and perhaps more thoroughly every two years. But it is also important to be continuously alert to any threats or problems."* Expert-3 adds the following to the governance of IT risk management: *"Policy-wise, it should be clear, so what I said at the beginning [IT risk management on strategic and tactical level] should be reviewed and updated periodically. This applies to risk analysis, business impact analysis, and determining measures to mitigate or accept risks. It is also important to have*

a good implementation of risk management and apply it periodically." Expert-2 thinks that there still is too little attention to security and privacy in risk management, *"So right there the whole risk management piece is very immature still though."*. The immaturity of IT risk management is mentioned by several Experts, housing association does manage their risks, but often the IT risks are an underexposed part (Expert 1,2,3 & 5). In the interview of case study participant-3 he mentions that the IT risk management policy dates back and has just been revised and formalized *"This [the newly formed policy] is going to be formally adopted soon and then there will be an annual cycle where these issues will be reviewed."*. At Wonen Zuid (case-study 2) is less than a year old and there is a revision scheduled *"Wonen Zuid formalized risk management policy is in place from the first quarter of 2022 and currently scheduled for review in the first quarter of 2023."* At Alwel (case-study 4) cyber risk is part of risk management, the interviewee of case-4 mentioned the following: *"We have a risk policy that includes cyber risks. We have identified the risks and this is periodically updated, with the last update in 2021."* At Stadlander (case-study 5) mentions that the risk management policy has not been updated, but plans are made to revise and further clarify the policy. The interviewee of case-5 tells the following about the risk management policy and the roles and responsibilities within the organization: *"We now find that that is not sufficiently embedded in the policy document. We have to start addressing this. That is actually what we have discovered from the audit, a lack of clarity in our organization."*

4.3.2 NIST framework

The NIST framework is mentioned in several interviews (Case study interviews 3&5, experts 1,2&3) and without mentioning the NIST framework as a whole, specific parts of this framework are mentioned in the other interviews as well. The NIST framework is a second-order theme, comprised of the following first-order codes: 'Identify', 'protect', 'detect', 'respond' & 'recover'.

At Stadlander, the NIST framework is used alongside the information security policy based on the BIC. The interviewee of case-5 says the following about the implementation of the NIST: *"1.5 years ago I said, well, this has to change. We see threats coming at us and we started using the NIST framework, the NIST cybersecurity framework. Based on that [NIST framework] we started taking all the measures to be ready for a cyber attack."* Together with external partners, Stadlander is working to fully implement the NIST framework. When asked about the total coverage of all IT risks at Stadlander, the interviewee of case-5 says the following *"Not yet. We are still in the process of development. [...] Both on identify, protect and detect we still need to make another step, but on respond we have made the extra step, with the business continuity plan. Most important still is the detect and recover, there we still need to take an additional step."* At Beveland Wonen (case-study 3), the NIST framework is also being used alongside the BIC. *"We do work with the NIST framework and we do expect to make further progress on that next year."* When asked about the reason why they use the NIST framework, the interviewee of case-3 responded the following: *"Because the NIST has a different perspective, the NIST is based on 5 pillars, [...]. And by working from those 5 pillars, you can start looking at your landscape in a much more focused way and see what measures you want to take."*

Different experts mentioned the NIST framework during the interviews. Expert-3 says the following: *"A NIST can help with creating a structured view of risks and the implementing of measures to mitigate them.* Expert-1 used the NIST framework during

a cooperation with different housing associations that work together, called ZWS. Expert-1 mentions the following: *"Many people were already familiar with ISO, but NIST was still unknown to them. We used the NIST at ZWS to raise awareness of NIST and to reflect on the current position of the individual housing associations and how it compares to others. This has helped them to become aware of the risks that may arise over time and what priority they should be given. So the NIST certainly is applicable."* Expert-2 and expert-3 both noticed the increase of usage of the NIST in the housing association sector. *"We see that the NIST is used by more and more. [...] or in combination with the ISO 27,000 series, so in terms of information security"* was said in the interview by expert-2. Expert 3 also recognizes an increase in the usage of the NIST framework, saying: *"More and more housing associations have also begun looking at the NIST cybersecurity framework, as it focuses more on cyber vulnerabilities and how to prevent, detect and remediate them."*

Different aspects of the NIST framework were mentioned by the participants of both the case-study interview and the expert interview. The identification ('identify' phase) of business processes, assets, and other resources needed for the continuity of the housing associations business, is mentioned by interviewees of case-2, case-3, expert 2 and expert 3. When talking about the lessons learned from a hack, expert 2 mentions the importance of identifying the different processes and assets in the organization, *"what processes and assets do we all have in place right now? Because if you don't know this, you can't secure it."*

The phase of 'protect' in the NIST framework is discussed in several interviews. For example the use of 'access control' is talked about by multiple participants, at Wonen Zuid a control mechanism called role-based access control (RBAC) is used. The interviewee of case-2 mentioned the use of RBAC when talking about information confidentiality: *"If a system is properly secured, you only get access based on your role. We use the "RBAC" (role-based access control) mechanism here. This means that we already check at the front end whether an employee may have access to a certain environment. Within this environment, it is then regulated what an employee may do there and to what extent they may do something. This is worked out very precisely for all employees, applications, functions, and cross-links between these elements."* At Alwel, a similar system is in place, the interviewee of case-4 says *"Access control is an important part of our processes"*. Also at Welbions, Beveland Wonen, and Stadlander a similar role-based system is used.

Detection is the least mentioned part of the NIST framework, during the interviews. Expert-2 states the following about the 'detect' phase: *"When it comes to detection, you just have to make sure you have the right monitoring in place to identify any suspicious activity in a timely manner."* In the case-study 5 interview, monitoring and detecting are notified as an area where improvement is needed. The following is said: *"Monitoring If it [a security breach] does happen. Well, there's still a big issue there of, how quickly do we notice that a hacker is inside anyway without an employee noticing it? [...] but that the system automatically detects it and takes measures. Well we still have to improve that aspect."*

The first-order code 'respond' is the aspect of the NIST framework theme that is mentioned the most during the case-study and expert interviews. *"I think before then [the hack at the beginning of 2022], less than 5% of corporations had an incident response plan what was current. I think that now about half of the associations will have one and that's still increasing very rapidly, so everybody received the wake-up call."* this is a quote from the interview with expert-3. In al the different case-study interviews, the response plan is

mentioned. In some of the cases they were finalizing the response plans, others already had them in place. The interviewee of case-4 adds on the matter: *"We need a response plan or a business continuity plan ready to go in case another crisis occurs so we can move quickly."* The importance of having a plan is underlined by expert-1, who says the following: *"It is also important to have a good crisis structure in order to respond efficiently. And to have clarity on who is allowed to do what in a crisis situation. What we have advocated in incident response plans, as they are there at the various housing associations, is that you have a structure (Covering: Imaging, Judgment and Decision Making). First you look carefully at what you know for sure, what you don't know and what you have doubts about (imaging). Secondly you look at what you assess as an organization (judgment). Afterwards follows the decision, which a chairman can make."*

The first-order code 'recover' is directly named in two case-study interviews and one expert interview, with expert 2. Where the following is said about the recovery phase of the NIST framework: *"Then arrive at recovery. [...] How are we going to recover things? Do we have plans in place for that as well? Can we recover at all, do we have backups, do we have a contingency environment in order to continue the processes that were interrupted?"* Expert-2 mentioned the recovery phase when being asked about the lessons learned from previous hacks. The interviewee of case-2 says the following about having a recovery plan: *"Being a housing associations, we carry a great risk with us right now, because even clicking on the wrong link can cause us all to be at risk. This means we need to be aware of our behavior and make sure we have recovery plans and a business continuity plan, with timelines and priorities for restoring our systems."* In the case-study interviews of case-1 and case-5 they both mention that their organisation is currently working on the recovery plan, or business continuity plan. Where the interviewee of case-5 explains that they are still looking for best practices in the area of recovery: *"But that (restoring back-ups) has a lot of implications for your recovery plan. You can't just restore one, because then you sync the new data into the system which has continued to work with the old data? There are still some challenges. I'm looking for best practices that we can use there."*

4.4 Privacy & information security

The aggregated dimension '*Privacy & information security*' is the combination of the second-order themes of '*CIA + PA*' and '*ISO / BIC*', as shown in figure 9.

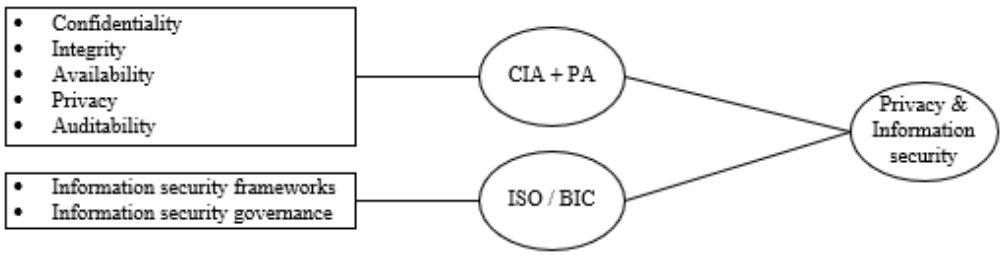

Figure 9
Privacy & information security in housing associations

4.4.1 Confidentiality, Integrity, Availability, Privacy & Auditability (CIA+PA)

The second-order theme of 'CIA + PA' is an abbreviation based on the CIA-triad ('confidentiality', 'integrity' & 'availability'), with the addition of 'privacy' and 'auditability'. The various first-order codes were discussed during all the case-study and expert interviews. During case-study interview 2, the following is said on the topic: *"To ensure that we can keep our information resources available to the organization and avoid being infected by viruses or ransomware, we need to monitor our business continuity. This means we must be aware of the most important aspects of information security: availability, integrity and confidentiality. If we don't know where the threats are coming from, we run the risk of being compromised."*

On the topic of the availability of information, expert-4 says the following: *"It is difficult to guarantee that your data will not be lost and that it will always be available. But by working with backups and storing the data in multiple places, you can guarantee that you can restore the data after a short downtime. But the more places you use to store the data, the more vulnerabilities you also create. There is always the risk that one of those places gets hacked."* In almost every case, when asked about the availability of the information a link is made with a service provider. In case-study 4, *"There are several procedures in place to ensure information security, such as making backups and using a backup service desk. We also cooperate with service providers to ensure that our systems are functioning properly and that we receive a defined service."* In cases 2,3 & 5 a similar answer is given. Expert-2 places a critical note about the responsibility, for the availability and service providers: *"The availability of your information systems and therefore for your data. The responsibility really does lie with whoever is responsible for it [within the organization or at the provider]. It's up to the associations to ask those questions to the provider, but too little happens."*

The importance of data integrity is noted in case-study 1: *"It is important to ensure the integrity of data through proper organization of lines [based on the 3-lines model] of control, including a second line and an auditor."* At Wonen Zuid (case 2) there are certain hard & soft controls in place to maintain data integrity, furthermore *"we have tight authorization schedules, where for each job function we determine exactly what access rights are assigned to the job profile based on the employee's role."* At Alwel (case 4), they have similar controls in place to maintain data integrity. At the case of Beveland Wonen (case 3) they also use authorization schedules, but C-3 says, *"People are given access to information based on their position. At the same time, Beveland Wonen's philosophy is that trust is placed in people's hands in the organization. That means a lot of information is accessible to everyone."* Expert-2 places a critical note on the usage of authorization schedules, keeping in mind the service providers who also use the IT systems. Expert-2 says the following: *"But again you have to deal with then your providers who also do certain stuff in those systems. They have admin rights and there's often a big risk there. [...] There is not enough grip on it [authorized access by both employees and the service provider] and not enough thought is given about the consequences of what if we have too many identities to have access. If we don't secure the access enough, we really run a big risk in terms of the integrity of the data because it could just be stolen or compromised."*

During the different interviews, the first-order code of 'confidentiality' is often discussed in terms of the preservation of authorized access and the limitation on the access and disclosure of information. The confidentiality of information is often secured by access control and multi-factor authorization (MFA), as was the case in

case-studies 1, 2, 3 & 5. In case 4 only access control is discussed. Experts 2 & 3 underline the usage of access control and MFA. Expert-3 adds the following on the importance of having proper access control in place: *"In a general sense, it is important that organizations take maximum measures to prevent the situation from spilling over to other [IT-]customer environments. This can be achieved by having proper authorizations and monitoring and by reacting quickly to unauthorized access to the system. The architecture of your network and signaling are very important. [...] This is also evidenced by reports of major hacks in the Netherlands, where municipalities and schools, for example, have also been affected."*

On the topic of the first-order code 'privacy' the GDPR was mentioned in all interviews, as discussed in subsection 4.2.3 on legislation. In a few case study and expert interviews some remarks were made about privacy in general (within housing associations). Expert-2 says the following about housing associations almost always comply with the GDPR, but still frequently take privacy into consideration during their every day processes and work. Expert-2 speaks about the privacy as follows: *"So how are we [as an organisation] going to protect the privacy? It frequently comes down to: "When things go wrong, the intervention will take place afterwards". Like "okay, we shouldn't do this anymore. Or should we? Or should we no longer record this kind of information?" "Well, We are now going to do a new, large-scale processing of data. I have sufficiently considered the privacy risks with a DPIA (Data Protection Impact Assessment)" for example, [...] But I think that's definitely the kind of thing that has taken years and is ongoing to really get that in place.* In the case-study 5, the participant sees a challenges when talking about privacy in his organisation: *"there is still one big challenge on piece of privacy. Also from a privacy point of view, we see that our systems have too much information that is still around. [...] Which is no longer relevant for our organisation to do business, but the information is there anyway."* Expert-5 talks about the same privacy-related problem, saying: *"In the past, the more information we [an organisation in general] had the better and we [the organisation in general] kept more historical data. Where we collected more information, it was important to keep everything. Over time we have incorporated certain mechanisms to clean up the data, but many associations still like to keep all the historical data."* In the case-study interview on Alwel, the interviewee of case-4 mentioned the following about the storage of data: *"During the hack we found that we still had a lot of data that was no longer functional and could be deleted. We now also have to make sure that we clean up the data and stay in the required time-frames; of course, we also have to keep data for tax purposes. In addition, privacy-sensitive data must be deleted faster. All of this must be done in a secure environment. The hack was a wake-up call for us to clean up within the systems."*

When talking about the previously discussed topics (CIA & Privacy), frequently the first-order code of the 'auditability' of the information systems was considered. In case-study interview 2,3,4 & 5 they use logging on their most important information systems. Where a record is made about who enters the system and who alters or mutates information in the system. When expert-2 is asked about the 'auditability' of information systems in housing associations, he replies the following: *"That's a question that will vary depending on each association per system, but in general you can assume that logging is being done. So that logging takes place on those systems and that and that that logging is also stored in a secure way."* Expert-2 continuous on the subject: *"But, preferably, you'd like to see periodic or perhaps continuous investigation of that [logging] based on a natural suspicious cases to irregularities. And in order to do so, you need monitoring."*

4.4.2 ISO / BIC

The first-order codes of 'information security frameworks' and 'information security governance' both are part of the second-order theme of 'ISO / BIC'. The five different cases all are familiar with the BIC as a information security framework. In all cases, the BIC framework is used. The interviewee of case-1 says the following about the BIC: *"The Baseline Information Security (BIC) is a standard to which risks and key performance indicators (KPIs) are linked. While it is not mandatory, it is recommended that we be compliant. We conducted a baseline measurement to determine what needs to be done to comply with the BIC. The BIC promotes awareness and helps to keep checking off what has been done to meet the standard. The BIC is the framework within which we work."* The interviewee of case-5 also mentioned the BIC: *"We have information security policies and plan in accordance with the BIC which is based on the ISO and is supplemented for housing associations. We have actually been using that one [the BIC] for years."*

The difference between the ISO and the BIC is identified by C-3: *"The difference between the ISO and the BIC is actually that the ISO prescribes a huge set of things without specifying, where the BIC really provides a baseline [for housing associations]"*. In the other case-studies, the BIC is also used in the organizations. At Wonen Zuid, the interviewee of case-2 mentioned the following: *"When looking at frameworks, at Wonen Zuid we look specifically at the ISO 27.000 series, specifically 27.001 and 27.002. With these, we determine our risk profile and the measures to mitigate it. We are also looking at other versions of these standards, to which the BIC 4.0 will also respond and anticipate developments such as chain automation, outsourcing, and SaaS. In fact, we are looking at the information security code from a broad perspective. In the latest version of the BIC, the fourth generation BIC from 2022, we are using the latest standards and norms prescribed in the directive."* The latest & revised version of the BIC, the BIC 4.0 is also mentioned in case-study 3 and is expected to be used in 2023.

Expert-1 sees the role of Aedes, the network organization promoting the interest of housing associations, in the usage of the BIC in housing associations: *"The BIC has been brought forward by Aedes, which I think is a good development."* All the experts talk about the importance of the ISO and BIC, however expert-3 and expert-5 notice that not many housing associations got an ISO certificate. Expert-4 also mentions the size of an organization in relation to the ISO, saying: *"I think the frameworks [ISO & NIST] are good but they still fall short for smaller organizations. For the smaller organizations, they are unworkable."* Also mentioning the factor of employers in the handling of the ISO framework, *"Indeed, while some frameworks, such as ISO certification, are good for defining processes in an organization, they do not guarantee that they will be acted upon. Because the individual employees ultimately perform actions, it is important that they are capable of acting and know what to do to mitigate cyber risks."*

When asked if privacy & information security are adequately embedded in the housing association sector, expert 5 responded as follows: *"I think it's important to tell that the about how I look at the situation. I didn't think it was very good about two to three years ago, but it has improved now. However, I still think it is only a meager six because the complexity is underestimated and people are quick to talk about accountability, while the willingness to invest in security is limited."* Expert-2 answers the same question by addressing the Plan Do Check Act (PDCA) cycles needed to keep the privacy & information security governance & policies up to date: *"I think that part [continuously revising the privacy &*

information security policies] is just very difficult. It often remains a one-time event or happens maybe once every few years." Expert-3 underlines the importance of periodically revising the privacy & information security policies.

When asked if privacy & information security are adequately embedded in their organization, the interviewee of case-2 says: *"The grade we give ourselves is sufficient but it remains an ongoing challenge to ensure that it remains sufficient. But we must always remain alert and prepared for any threats. If we face a major attack where we are heavily compromised, we have our response plans ready."* At the case-study interview of case-3, the response is similar: *"I think so. Because we have it [privacy & information security] adequately In the sights. [...] at this moment it is adequately guaranteed. But that doesn't mean that there is nothing to improve."* The interviewee of case-4 gives the following answer: *"There are always areas for improvement, and it is only natural to want to reach for the highest level. But sometimes it is also important to consider whether it is still workable [for the employees]. [...] right now, the privacy & information security is adequately guaranteed."* The interviewee of case-5 also mentions that his organization is in control, but also stresses the importance of privacy & information security awareness in organizations. When asked about if privacy & information security are adequately embedded in the housing association sector, the interviewee of case-1 answers: *"No, [...] as I said, even the best organizations can be hacked."*

5 Discussion, limitations, conclusion, and recommendations

5.1 Discussion

Privacy & information security are getting increasingly important in the continuously evolving cyber threat landscape. For the Dutch housing association sector to better protect itself against the cyber vulnerabilities that are out there, a privacy & information security approach to IT risk management is proposed in this thesis. This thesis aims to explore how different factors influence IT risk management in the housing association sector, moving towards a privacy & information security framework. To take a deeper understanding of the different factors, the participants in this research were asked to share their knowledge of different factors. The various factors are internal variables, external developments, IT risk management, and privacy & information security in the Dutch housing association sector. To further evaluate the participants' perspectives on the different topics, the academic perspective on the factors is taken into consideration. Therefore, this chapter discussed the combination of the results from the case-study interviews, the expert- interviews, and the theory about the factors and their influence in the Dutch housing association sector.

5.1.1 Internal variables in the Dutch housing association sector

The results on the relationship between a housing association and cyber vulnerabilities, when looking at the internal variables, is a triangle framework, composed of 'People', 'Processes', and 'Technology'. This triangle framework is also shown in the research by Dhillon et al. (2021). Where Dhillon et al. (2021) state that to explore security threats, vulnerabilities and risk, and to identify risk management strategies the socio-technical perspective could be used. The socia-technical perspective being people, processes, and technology (Tanriverdi & Du, 2020). These three terms are used to answer the first sub-research question: *"What are the internal variables when it comes to organizational cyber-vulnerabilities in the Dutch Housing Association Sector?"*

The part of people, analysis shows that different concerns are important to keep in mind. At first the item of responsibility in a housing association, where the ultimate responsibility rests in the hands of the executive board. The board often delegates the responsibility for cyber-security to the organizations and managers, and the responsibility for privacy & information security is frequently laid in the hands of the privacy and security officers. As partially in line with the report written by the national Cyber Security Centre Netherlands (2020) on 'Risk Management', where the role of the board is one of managing information as an agent of the product (like capital) and promotes this point of view among the whole organization. Furthermore, according to the national Cyber Security Centre Netherlands (2020), the board is responsible and will be held accountable in case of an information-related incident which is also the case in housing associations. However, the results and report of the NCSC-NL show that an organization-wide feeling of being responsible, from the top down is needed. This feeling of organization-wide responsibility should be promoted by the board, which is not yet the case at housing associations according to the results.

Furthermore, a clear distribution of those responsibilities should be written down in the IT risk management and privacy & information security policies, which should be approved by the board. Providing a clear and standardized overview of which

roles in the organization are responsible. The by the board approved risk management, privacy & information security policies is in line with the report on Risk management by the national Cyber Security Centre Netherlands (2020). Secondly, a focus on the awareness of all employees, on the aspects of privacy & information security, and cyber threats, should be kept. The results from the case-studies and expert interviews are in line with the theory of Sohrabi Safa et al. (2016). Where Sohrabi Safa et al. (2016) says that employees' information security awareness plays a vital role in an organizations defence against information security breaches. Furthermore, according to Mee & Brandenburg (2020), around 95% of cybersecurity issues can be traced back to human error, further showing the importance of awareness. The NCSC-NL adds that an organization should create clear instructions on how to work with information, something that is not always the case at housing associations. Moreover, the NCSC-NL underlines the importance of creating awareness among employees, especially around important and sensitive information. The provision of training courses and awareness campaigns should help create this awareness, as also seen in the results. Thirdly, next to the awareness of employees, the IT, privacy & information security knowledge in the organization is important to keep in mind. The role of the CISO or more frequently used in housing associations, the security officer, is one which could be further evaluated. As it should be a role that gives advice on information security, coordinates the information security tasks, and audits the information security (national Cyber Security Centre Netherlands, 2020). Housing associations should evaluate whether the role of the security officer is one of advice, coordination, and internal audits in their organization. The role of the privacy officer should be of similar competence, but with regard to privacy.

When looking at the processes, the results show the dependency of the housing associations on their IT landscape. Many important business processes, tools, and applications rely on IT to keep the business going. But the IT landscape in housing associations is one where IT is frequently outsourced, along with the knowledge of IT. However, it is important to keep responsibility and control over the entire, internal and external, IT landscape. The directorial role towards the IT providers is one that housing associations should keep, as well as good communication and agreements with the provider. A risk-minded approach could help to discover gaps in communicative lines, agreement, or division of responsibilities between the housing association and the IT provider.

Less attention is given to the technology aspect of information security during this research. Where the results show that there are a lot of different technical security tools and protocols available to protect the housing associations, making the technology aspect an important factor in risk mitigation. The balance between the security aspect and workability is an aspect to keep in mind.

These results give new insights into how a clear division of responsibility, not only between the board, managers, and employees, but also between the organization and their (IT-) partners influences privacy & information security. Furthermore, the data contributed a clearer understanding of how awareness among employees in housing associations needs a strong focus, because *"the most important firewall is just sitting between the monitor and the chair"* (Case-study interviewee 3). People are an important part of the cyber security in a housing association. In addition, the IT knowledge and expertise in housing associations, influence the ability of a housing association to limit

cyber vulnerabilities. The results on people, processes, and technology, should be taken into account when discussing the internal variables of cyber vulnerabilities and the Dutch housing association sector.

5.1.2 External development in the Dutch housing association sector

The results on the relationship between a housing association and cyber vulnerabilities, when looking at the external developments, mentioned the following themes: 'cyber threats', 'cyber security assistance', and 'legislation'. These three themes are discussed to answer the second sub-research question: *"What are the external developments when it comes to cyber-vulnerabilities in the Dutch housing association sector?"*

The results of the external developments indicate that the different cyber attacks that happened in the housing association sector, along with the damage the cyber-attacks inflicted, make housing associations aware of the growing cyber threat. However, what is not frequently around, is a structured way of keeping informed on cyber threats and the evaluation of how the cyber threats influence the organization. Furthermore, the cooperation between individual housing associations on the topic of cyber security, as well as a sector-wide approach to cyber security could be further evaluated, as there are chances to share knowledge and experiences, which could positively influence the overall cyber resilience of the Dutch housing association sector. Another factor that influences the cyber resilience of the Dutch housing association sector is the cooperation between housing associations and external partners in the area of cyber security. This cooperation aims at, on the one hand, the gathering of information on the cyber threat landscape. On the other hand, the cooperation aims to fill in the need for assistance on cyber security, at different levels of the organization.

The results show that the GDPR, which has been introduced in 2018, had a positive impact on privacy and data protection in housing associations. Where all organizations need to comply with the legislation, which caused different housing associations to give more attention to the topic of privacy. Resulting in, for example, the creation of privacy expert groups and the introduction of a 'privacy officer' role in the organizational structure of housing associations.

The results of the external developments give insights into how the housing association sector keeps track of cyber threats, uses cyber security assistance, and coops with privacy and data protection legislation. Similarities can be found between the results of this research and the "Dutch Cybersecurity strategy 2022-2028", which discusses the ambitions and plans for a safer digital society (national Cyber Security Centre Netherlands, 2022). The sector-wide cooperation in the area of cyber security, where leading organizations provide a teaching role towards their specific sector, is a part of the Dutch cybersecurity strategy that could also be further investigated for the Dutch housing association sector. Further cooperation between housing associations and a sector-wide approach on the topic of cyber security, in which sector-specific knowledge, experiences, and assistance are provided, will positively influence the sector's ability to deal with cyber vulnerabilities. Furthermore, the sight and understanding of the different cyber threats, are mentioned as one of the focal points of the Dutch Cybersecurity strategy. The sight of, and understanding of, threats can also help associations, but the link between the external threat as an influence on IT

risk and the management of those risks should be further evaluated.

5.1.3 IT risk management in the Dutch housing association sector

To explore how IT management could be used in the Dutch housing association sector, first, the current situation needs to be discussed. Furthermore, the influence that the use of risk management framework in the housing association sector could have, is evaluated. This section will answer the following sub-research question: *"To what extend is IT risk management being used in the Dutch housing association sector in order to manage cyber-vulnerabilities?"*

When it comes to digital vulnerabilities, risk management is still in its infant stage, according to the NCTV (for Counter-terrorism & Security, 2022). The results on IT risk management in the Dutch housing association sector indicate that housing associations are in the early phases of transition when it comes down to managing IT risk, and becoming aware of the importance of managing IT risk. The hack on different housing associations at the beginning of 2022, was a wake-up call to the sector as a whole. Where housing associations are evaluating their IT risk management and improving the different stages of the risk management process, as described by Refsdal et al. (2015) in their book on 'Cyber-Risk Management'. In the theory on cyber-risk management, Refsdal et al. (2015) mentions the importance of risk management is based on a risk management framework, which should act in accordance with risk management principles. Both the principles and the framework must be decided upon by the overall management of an organization, or in the case of housing associations: the executive board, together with management. Where the management should safeguard the risk management process, consisting of 'communication & consultation', 'monitoring & review', and 'risk assessment'. The first two stages should happen in a continuous fashion, and the risk assessment is done routinely. The same stages as described by Refsdal et al. (2015), are used in the ISO 27005 framework, making the ISO 27005 a useful tool that is not yet used frequently in a housing association.

The results suggest that the housing associations are currently focused on the 'risk assessment' stage of the process when it comes to IT risk management. Trying to get a hold of the IT risk by aiming to understand and document these risks. The assessment results serve as a decision basis for risk management, including the decision on the controls and measures needed to mitigate the risk (Refsdal et al., 2015). The same concerns housing associations, who use the IT risk assessment stage as a decision basis in their organization. The focus on the IT risk assessment, should not mean that less attention is given to the other two stages in the risk management process. First the communication and consultation stage, the stage which aims at the sharing, obtaining, and provision of information on the IT risk. Furthermore, the stage aims at the interaction between different stakeholders regarding the management of risk (Refsdal et al., 2015). For this stage to be effective, Refsdal et al. (2015) advise the establishment of a dedicated team and define a plan for the process. The creation of a dedicated team, or expert group to evaluate the IT risks in an organization, is also discussed in the results. Where multiple interviewees mentioned the importance of a multidisciplinary group, which frequently evaluates IT risks. The focus of the dedicated team should also be on ensuring the endorsement of the risk management process. *"Effective and efficient management of risk requires decision-makers, stakeholders, and any key personnel to pull in the same direction"* Refsdal et al., 2015, p.13. The results show that the level at which

communication and consultation happen at housing associations when discussing IT risk management varies and does not frequently happen in a standardized fashion.

The 'monitoring and review' stage in the theory by Refsdal et al. (2015) is divided into two important aspects. The first is the monitoring and reviewing of risks and the second is the monitoring and reviewing of risk management. When looking at IT risk management, the first part includes the monitoring of organizational IT assets, threats, vulnerabilities, and the impact those vulnerabilities could have. This kind of monitoring creates a link to the external developments discussed in section 5.2. The second is needed to ensure that the IT risk management framework and process remain relevant and adequate. Furthermore, the risk evaluation criteria should also be reviewed from time to time. The results indicate that the way housing associations monitor and review IT risks, and IT risk management differs. Overall the monitoring and reviewing of IT risk and IT risk management still plays a limited part when talking about IT risk management at Dutch housing associations.

The results show that the use of the NIST framework or ISO 27005 standard could provide the necessary handles for housing associations to grab a hold of IT risk management in their organization. Because both frameworks could help create a structured view of IT risks, and IT risk management. The results show that the use of the NIST framework is increasing. However, also with the use of the frameworks the aspects of 'monitoring and reviewing', and 'communication and consolation' should be as important as the 'risk assessment' part. Keeping in mind the dynamic nature of IT risks.

5.1.4 Privacy & information security in the Dutch housing association sector

To evaluate how privacy & information security are influenced in the Dutch housing associations sector, the topics of privacy & information security are discussed in this section. This section will answer the fourth and last sub-research question: *"What role does privacy & information security play in the Dutch housing association sector in order to manage the cyber-vulnerabilities?"*

Information security can be explained by using the security triad, or in other words, the CIA triad (Pfleeger et al., 2015). The protection against unauthorized access, use, disruption, modification, disclosure, or even destruction, to provide the confidentiality, integrity, and availability of information in an organization (Kissel, 2013). The results show that policies on how to secure information exist in housing associations, where different ways are used in order to secure confidentiality, integrity, and availability in their organization. In all the cases the Baseline Information Security Housing Association (BIC), which is an ISO-based framework, is used to create an information security baseline to safeguard the CIA. However, according to ISO 27002, to adopt a standard an organization must first determine its own security requirements. Requiring an organizational risk assessment, the legal requirements, and a set of principles, objectives, and business requirements (ISO, 2022b).

The results discuss the legal requirements, set of principles, and business requirements of housing associations. Where the legal requirements are in the GDPR, when talking about information. The set of principles used is frequently confidentiality, integrity, and availability. Where the principles of 'privacy' and 'auditability' could

be added, when securing privacy-sensitive data. Information security and business requirements can often be a balancing act between having the best security and still being workable for employees. Furthermore, the risk assessment part of using an information security framework is an important link to IT risk management in an organization. In order to discuss, implement and continuously improve IT risk management, a housing association requires to use the risk management process for information technology risk. Fully implementing the process, with the creation of a cycle where IT risk assessments, along with communication, consultation, and the continuous monitoring and reviewing of the process and risks, is important for privacy & information security in a housing association. Keeping in mind the information security principles of confidentiality, integrity, availability, privacy, and auditability.

With the BIC, housing associations create an information security baseline on which they try to comply. Important to keep in mind is that the information technology risks influencing information security are not static factors. The IT risks are dynamic and constantly evolving, and this is also the case in the housing association sector. The findings imply that, where housing associations do focus on privacy & information security, they should more frequently do this from a viewpoint where IT risks are dynamic and thus should be constantly monitored and reviewed, as well as the entire IT Risk Management Process.

5.2 Limitations

The qualitative and exploratory nature of this research presents several research limitations. There is the question of validity or credibility (Stebbins, 2001), and reliability in this research. Multiple limitations shall be discussed.

Starting with the limitations of the case-study research. On the topic of validity, several limitations could affect the research. There could be a lack of generalizability, as five different housing associations participated in the case study research. The total number of housing associations in the Netherlands is around 300 (WerkenAanWonen, 2022), so there is a risk of sampling bias because of the limited sample size. However, the external validity is improved by using expert interviews, where four out of the five experts are operating in the housing associations sector. For example, company expert 5 is an employee, who works with over 200 different housing associations. Furthermore, expert 2 and expert 3 work at a company that helps housing associations in their digital transition. They have been providing this help and advice to the housing association sector for more than 15 years.

The cases are selected through the network of the researcher's company supervisor, which could lead to a selection bias. Where the housing associations used in the case study could possibly be selected because of their interest in the topic or because they were already working on the different topics in the research. Next to the selection bias, there is always a risk of respondent bias; unfortunately, no data triangulation was achieved to mitigate the respondent bias. The decrease in external validity, because of possible selection and respondent biases, is addressed with expert interviews and clear selection criteria for both the case study participants and the experts who participated in the research.

Concerning the inductive thematic data saturation model, the emergence of new first-order codes throughout the analysis phase became lesser but was not fully achieved. Due to the time constraint of the research, no further case studies or interviews could be completed. The interviews were conducted in Dutch and open-ended questions were asked, allowing the participants to express themselves fully. However, the research is written in English, and the relevant quotes, as well as the transcript, were translated from Dutch to English. This could potentially influence the study's validity. Several strategies are employed to ensure the high validity of the research and limit the researcher's bias. Strategies such as transcribing immediately after an interview, sending the transcript to the participants to receive feedback, the usage of low-inference descriptors (with direct quotations), and having the research reviewed by peers.

As for the reliability of the research, a clear way of documenting the methods, measures, tools, and data analysis structure can be found in chapter 3. Reliability depends on explicitly describing the observational procedures (Kirk & Miller, 1986). However, there is always the concern of reproducibility across codes, also called inter-coder reliability (Campbell et al., 2013). The concern is whether different researchers would code the data the same way. In order for others to make it easier to code data the same way, the data analysis structure is used. The data analysis structure tries to add to the reliability of the research.

5.3 Conclusion and recommendations

"Guided by the precept that to understand any phenomenon well, it is necessary to start by looking at it in broad, nonspecialized terms" (Stebbins, 2001). This research, which has an exploratory nature, is conducted with the aim of better understanding how IT risk management, privacy & information security, and cyber vulnerabilities relate to each other within the Dutch housing association sector. This research aims at answering the following research question:

"How could Dutch housing associations use IT risk management in order to manage their cyber-vulnerabilities?"

The different aspects of the internal variables, external developments, privacy& information security all have a role to play in answering the main research question. This research gives insights into the different topics. Furthermore, this research shows how the aspects relate to each other, and IT risk management, within the context of the Dutch housing association. An overview of how the different topics related to each other within the context of Dutch housing associations can be found in figure 10. The sector-specific framework shows the interplay between IT risk management and the different aspects that influence or are influenced by cyber vulnerabilities.

For Dutch housing associations to manage their cyber vulnerabilities using IT risk management, a few things must be kept in mind. At first, 'people, processes and technology,' or the internal variables, are aspects that need focus. Where all three are important, special attention should be given to a clear division of responsibility in the organization, the IT knowledge and expertise in the organization, and the awareness among all employees on the topic of privacy & information security.

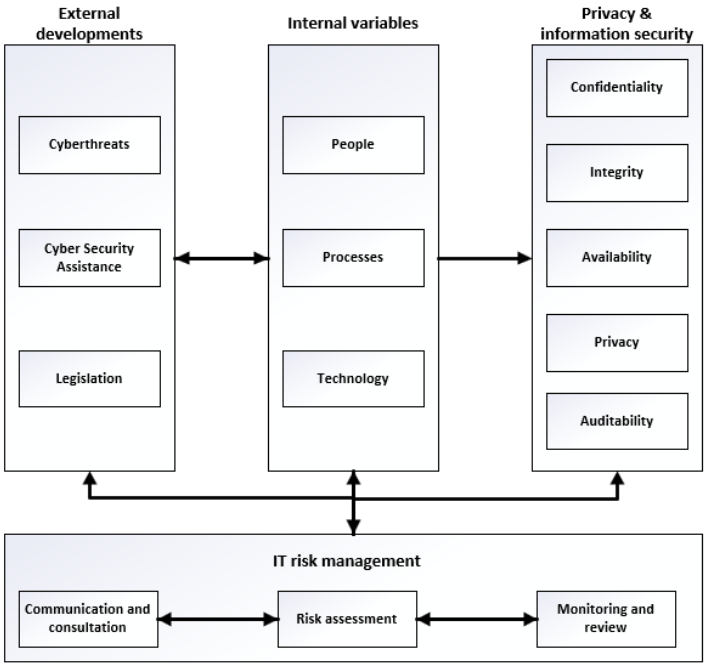

Figure 10
Towards a sector specific 'privacy & information' security framework

Secondly, for a housing association, it is important to get a grip on the external developments that influence IT risk management and the organization. To manage cyber vulnerabilities, a structured way of keeping informed on the different cyber threats and evaluating the threats and their impact on the organization is needed. Furthermore, cooperation between individual housing associations, as well as cooperation in the entire Dutch housing associations sector, will positively influence the sector's ability to deal with cyber vulnerabilities. Where all housing associations will profit from the sharing of sector-specific knowledge and experiences.

The third aspect is privacy & information security in a housing association. An aspect that is influenced by both internal variables is IT risk management. The BIC provides the housing association sector with a baseline for their information security, nevertheless, it is important to keep in mind that the risks that threaten both privacy & information security are dynamic and constantly evolving. Privacy & information security, therefore, need continuous management of the IT risk to keep up. Doing an organizational risk assessment is the first step toward defining how privacy & information could be secured in a housing association. However, a lasting impact can be made by creating a continuous way of dealing with 'monitoring and reviewing' and the 'communication and consultation' phases. The introduction of frameworks like the NIST and ISO 27005 could provide helpful tools and necessary handles for housing associations to grab a hold of IT risk management in their organization.

In conclusion, this research gives a clear first impression of the different aspects to consider when discussing IT risk management and the Dutch housing association

sector. It provides an overview of how the various topics relate, based on the study's results (figure 10). For further research, it is recommended to widen the sample to more housing associations. For example, an additional survey across the entire sector could help achieve additional external validity. Furthermore, supplementary research is needed to further evaluate and elaborate the sector-specific 'privacy & information security' framework. Moreover, future studies should also be aimed at the different individual topics discussed in this research. Taking a deeper dive into the different unique aspects of the housing association sector. Many studies must be undertaken to generate a valid, sector-wide theoretical framework. At last, future research could aim to discover the best practices for IT management, privacy, and information security in sectors similar to the Dutch housing association sector. Sectors of interest could be the healthcare sector or the educational sector. Both sectors provide services to specific populations in Dutch society, such as low-income or vulnerable individuals, and could face similar privacy & information security problems. Furthermore, investigating how these best practices could benefit the Dutch housing association sector is an exciting area for future research.

Bibliography

References

(n.d.).

Accenture. (2022, 2). *Threats Unmasked* (Tech. Rep.). Retrieved from https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf

Agrawal, V. (2017, 6). A Framework for the Information Classification in ISO 27005 Standard. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. Retrieved from http://dx.doi.org/10.1109/cscloud.2017.13 doi: 10.1109/cscloud.2017.13

Alzahrani, S., Xiao, Y., & Sun, W. (2022). An Analysis of Conti Ransomware Leaked Source Codes. *IEEE Access*, *10*, 100178–100193. Retrieved from http://dx.doi.org/10.1109/access.2022.3207757 doi: 10.1109/access.2022.3207757

Atos. (2022, 7). *Raison d'être.* Retrieved from https://atos.net/en/raison-detre

Bailey, D. E., Faraj, S., Hinds, P. J., Leonardi, P. M., & von Krogh, G. (2022, 1). We Are All Theorists of Technology Now: A Relational Perspective on Emerging Technology and Organizing. *Organization Science*, *33*(1), 1–18. Retrieved from http://dx.doi.org/10.1287/orsc.2021.1562 doi: 10.1287/orsc.2021.1562

Barnes, S. J., & Vidgen, R. T. (2006, 9). Data triangulation and web quality metrics: A case study in e-government. *Information amp; Management*, *43*(6), 767–777. Retrieved from http://dx.doi.org/10.1016/j.im.2006.06.001 doi: 10.1016/j.im.2006.06.001

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021, 12). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers amp; Security*, *111*, 102490. Retrieved from http://dx.doi.org/10.1016/j.cose.2021.102490 doi: 10.1016/j.cose.2021.102490

Brumfield, C., Haugli, B., & Sons, J. W. . (2021). *Cybersecurity Risk Management*. Hoboken, NJ, Verenigde Staten: Wiley.

Campbell, J. L., Quincy, C., Osserman, J., & Pedersen, O. K. (2013, 8). Coding In-depth Semistructured Interviews. *Sociological Methods amp; Research*, *42*(3), 294–320. Retrieved from http://dx.doi.org/10.1177/0049124113500475 doi: 10.1177/0049124113500475

CBS. (2021, 8). *8 miljoen woningen in Nederland.* Retrieved from https://www.cbs.nl/nl-nl/nieuws/2021/31/8-miljoen-woningen-in-nederland

Cherdantseva, Y., & Hilton, J. (2013, 9). A Reference Model of Information Assurance amp;amp;amp; Security. *2013 International Conference on Availability, Reliability and Security*. Retrieved from http://dx.doi.org/10.1109/ares.2013.72 doi: 10.1109/ares.2013.72

Cherdantseva, Y., Hilton, J., Rana, O., & Ivins, W. (2016, 11). A multifaceted evaluation of the reference model of information assurance amp; security. *Computers amp; Security*, *63*, 45–66. Retrieved from http://dx.doi.org/10.1016/j.cose.2016.09.007 doi: 10.1016/j.cose.2016.09.007

Company, T. S. (2022, 4). *The Sourcing Company - Prettig werken in de cloud.* Retrieved from https://thesourcingcompany.nl/en/

CORA. (n.d.). *Gegevenshuishouding - Woningcorporatie Referentiearchitectuur (CORA).* Retrieved from https://cora.wikixl.nl/index.php/Gegevenshuishouding

CorpoNet. (2022, 1). *BIC*. Retrieved from https://corponet.nl/producten/bic/

Crabtree, B. F., & Miller, W. L. (1999). *Doing Qualitative Research* (2nd ed.). SAGE Publications. Retrieved from https://books.google.nl/books?hl=en&lr=&id=4ebxYPyY5noC&oi=fnd&pg=PR9&ots=7B669aUyPH&sig=2sB10aYg1UWqPDoby0ndCMOn-Ec&redir_esc=y#v=onepage&q&f=false

Davis, E., & Mee, P. (2021). *Growing Cyber Threat Demands a United Response.* Retrieved from https://www.marshmclennan.com/insights/publications/2021/october/growing-cyber-threat-demands-a-united-response.html

de Jong, W. (2022a, 4). Gevolgen van hack bij L'Escaut stelt geduld van huurders op de proef. Retrieved from https://www.pzc.nl/walcheren/gevolgen-van-hack-bij-lescaut-stelt-geduld-van-huurders-op-de-proef~aa9b53e3/

de Jong, W. (2022b, 10). Oplichters bestelen Vlissingse ouderen, mogelijk verband met datalek bij woningcorporatie L'Escaut. Retrieved from https://www.pzc.nl/zeeuws-nieuws/oplichters-bestelen-vlissingse-ouderen-mogelijk-verband-met-datalek-bij-woningcorporatie-lescaut~ad19d38b/?referrer=https%3A%2F%2Ft.co%2F

Dhillon, G., Smith, K., & Dissanayaka, I. (2021, 12). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, *30*(4), 101693. Retrieved from http://dx.doi.org/10.1016/j.jsis.2021.101693 doi: 10.1016/j.jsis.2021.101693

DiCicco-Bloom, B., & Crabtree, B. F. (2006, 4). The qualitative research interview. *Medical Education*, *40*(4), 314–321. Retrieved from http://dx.doi.org/10.1111/j.1365-2929.2006.02418.x doi: 10.1111/j.1365-2929.2006.02418.x

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. Retrieved from http://dx.doi.org/10.4236/jis.2013.42011 doi: 10.4236/jis.2013.42011

Drost, E. (2011, 1). Validity and reliability in social science research. *Education research and perspectives*, *38*(1), 105–123.

Engelaar, R. (2022, 3). *Onduidelijk hoeveel informatie de hackers bij deltaWonen hebben buitgemaakt.* Retrieved from https://www.rtvoost.nl/nieuws/2080001/onduidelijk-hoeveel-informatie-de-hackers-bij-deltawonen-hebben-buitgemaakt

Etikan, I., Musa, S., & Alkassim, R. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1. Retrieved from http://dx.doi.org/10.11648/j.ajtas.20160501.11 doi: 10.11648/j.ajtas.20160501.11

Faik, I., Barrett, M., & Oborn, E. (2020, 9). How Information Technology Matters in Societal Change: An Affordance-Based Institutional Perspective. *MIS Quarterly*, *44*(3), 1359–1390. Retrieved from http://dx.doi.org/10.25300/misq/2020/14193 doi: 10.25300/misq/2020/14193

Fainmesser, I. P., Galeotti, A., & Momot, R. (2022, 8). Digital Privacy. *Management Science*. Retrieved from http://dx.doi.org/10.1287/mnsc.2022.4513 doi: 10.1287/mnsc.2022.4513

for Counter-terrorism, D. N. C., & Security. (2022, 10). *Nederlandse Cybersecuritystrategy 2022-2028* (Tech. Rep.). Retrieved from https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022---2028

Friese, S. (2012). Qualitative Data Analysis with ATLAS.ti. *SAGE Publications Ltd*. Retrieved from http://dx.doi.org/10.4135/9781529799590 doi: 10.4135/

9781529799590
Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012, 7). Seeking Qualitative Rigor in Inductive Research. *Organizational Research Methods*, *16*(1), 15–31. Retrieved from http://dx.doi.org/10.1177/1094428112452151 doi: 10.1177/1094428112452151
Goguen, A., Feringa, A., & Stoneburner, G. (2002). Risk management guide for information technology systems :. *Computer Security*. Retrieved from http://dx.doi.org/10.6028/nist.sp.800-30 doi: 10.6028/nist.sp.800-30
Golafshani, N. (2015, 1). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*. Retrieved from http://dx.doi.org/10.46743/2160-3715/2003.1870 doi: 10.46743/2160-3715/2003.1870
Groenendijk, M. (2022, 5). *Hoe een beruchte Russische cyberbende binnendrong bij woningcorporaties: 'Vroegen absurd hoog bedrag'*. Retrieved from https://www.bndestem.nl/dordrecht/hoe-een-beruchte-russische-cyberbende-binnendrong-bij-woningcorporaties-vroegen-absurd-hoog-bedrag~a474c0cf/?cb=50543f6637f506f327e06232f01c0d3e
Helderman, J. (2007, 1). De corporatie: tussen status en contract. SEV-essay ten behoeve van het project Vernieuw(d) Maatschappelijk Onderschap. *SEV*. Retrieved from http://repository.ubn.ru.nl/bitstream/handle/2066/46506/46506.pdf
ISO. (2018, 2). *ISO 31000:2018* (Tech. Rep.). Retrieved from https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en
ISO. (2021, 6). *Standards.* Retrieved from https://www.iso.org/standards.html
ISO. (2022a, 10). *ISO/IEC 27001:2022.* Retrieved from https://www.iso.org/standard/82875.html
ISO. (2022b). *ISO/IEC 27002:2022.* Retrieved from https://www.iso.org/standard/75652.html
ISO. (2022c). *ISO/IEC 27005:2022.* Retrieved from https://www.iso.org/standard/80585.html
Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016, 6). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954–2965. Retrieved from http://dx.doi.org/10.1111/jan.13031 doi: 10.1111/jan.13031
Kaplan, B., & Duchon, D. (1988, 12). Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study. *MIS Quarterly*, *12*(4), 571. Retrieved from http://dx.doi.org/10.2307/249133 doi: 10.2307/249133
Kirk, J., & Miller, M. (1986). Reliability and Validity in Qualitative Research. *SAGE Publications, Inc.*. Retrieved from http://dx.doi.org/10.4135/9781412985659 doi: 10.4135/9781412985659
Kissel, R. (2013, 5). Glossary of key information security terms. *National Institute ofStandards and Technology*. Retrieved from http://dx.doi.org/10.6028/nist.ir.7298r2 doi: 10.6028/nist.ir.7298r2
Koopman, M., Straub, V. M., , Mossel, V., & Straub, A. (2009a). *Performance Measurement in the Dutch Social Rented Sector: Volume 19 Sustainable Urban Areas*. IOS Press.
Koopman, M., Straub, V. M., , Mossel, V., & Straub, A. (2009b). *Performance Measurement in the Dutch Social Rented Sector: Volume 19 Sustainable Urban Areas*. IOS Press.
Koopman, M., van Mossel, H.-J., Straub, A., & van Mossel, H. (2008). *Performance Measurement in the Dutch Social Rented Sector*. Amsterdam, Nederland: Amsterdam University Press.
Lee, I. (2021, 9). Cybersecurity: Risk management framework and investment cost

analysis. *Business Horizons*, *64*(5), 659–671. Retrieved from http://dx.doi.org/10.1016/j.bushor.2021.02.022 doi: 10.1016/j.bushor.2021.02.022

Leonardi, P. M. (2020, 10). COVID-19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence in the Wake of Remote Work. *Journal of Management Studies*, *58*(1), 249–253. Retrieved from http://dx.doi.org/10.1111/joms.12648 doi: 10.1111/joms.12648

Levy, Y., & J. Ellis, T. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: The International Journal of an Emerging Transdiscipline*, *9*, 181–212. Retrieved from http://dx.doi.org/10.28945/479 doi: 10.28945/479

Mee, P., & Brandenburg, R. (2020, 12). *After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk.* Retrieved from https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education

ministry-of Justice, & Security. (2022, 8). *Cybersecuritybeeld Nederland 2022.* Retrieved from https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland

ministry of the Interior, & Relations, K. (2021, 5). *Housing associations.* Retrieved from https://www.government.nl/topics/housing/housing-associations

ministy-of-the-Interior-and Kingdom-Relations, & Aedes. (2022, 6). *National performance agreement* (Tech. Rep.). Retrieved from https://aedes.nl/media/document/volledige-tekst-nationale-prestatieafspraken

Monternie, A. (2022). *Acht woningcorporaties weigeren losgeld te betalen.* Retrieved from https://www.computable.nl/artikel/nieuws/security/7338989/250449/acht-woningcorporaties-weigeren-losgeld-te-betalen.html

Motii, A., Hamid, B., Lanusse, A., & Bruel, J.-M. (2015, 7). Guiding the selection of security patterns based on security requirements and pattern classification. *Proceedings of the 20th European Conference on Pattern Languages of Programs*. Retrieved from http://dx.doi.org/10.1145/2855321.2855332 doi: 10.1145/2855321.2855332

Mousavi Baygi, R., Introna, L. D., & Hultin, L. (2021, 1). Everything Flows: Studying Continuous Socio-Technological Transformation in a Fluid and Dynamic Digital World. *MIS Quarterly*, *45*(1), 423–452. Retrieved from http://dx.doi.org/10.25300/misq/2021/15887 doi: 10.25300/misq/2021/15887

national Cyber Security Centre Netherlands. (2020, 9). *Risk management: the value of information as point of departure.* (Tech. Rep.). Retrieved from https://english.ncsc.nl/publications/factsheets/2020/september/15/factsheet-risk-management-the-value-of-information-as-point-of-departure

national Cyber Security Centre Netherlands. (2022, 10). *NCSC-NL Research Agenda 2023 – 2026* (Tech. Rep.). The Hague, nl. Retrieved from https://english.ncsc.nl/publications/publications/2022/october/11/ncsc-research-agenda-2023-2026

Naumann, M., & Van Weersch, m. (2022). *âHelft van onze huurders is niet-digitaal vaardigâ.* Retrieved from https://www.aedesmagazine.nl/edities/3-2022/artikelen/helft-van-onze-huurders-is-niet-digitaal-vaardig

netwIT-and-FLOW-and Aedes. (2011, 12). *CORA 3.0* (Tech. Rep.).

O'Neil, I., Ucbasaran, D., & York, J. G. (2022, 1). The evolution of founder identity as an authenticity work process. *Journal of Business Venturing*, *37*(1), 106031. Retrieved from http://dx.doi.org/10.1016/j.jbusvent.2020.106031 doi: 10.1016/

j.jbusvent.2020.106031
Pfleeger, C., Pfleeger, S., & Margulies, J. (2015). *Security in Computing* (5th ed.). Pearson.
Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-Risk Management (SpringerBriefs in Computer Science)* (1st ed. 2015 ed.). Springer.
Ross, R. S. (2018, 12). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. *Special Publication (NIST SP) - 800-37 Rev. 2*. doi: 10.1002/https:/doi.org/10.6028/nist.sp.800-37r2
Sanders, R. (2022, 3). *The Sourcing Company en klanten in last door hack.* Retrieved from https://www.computable.nl/artikel/nieuws/security/7336924/250449/the-sourcing-company-en-klanten-in-last-door-hack.html
Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., ... Jinks, C. (2017, 9). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality amp; Quantity*, *52*(4), 1893–1907. Retrieved from http://dx.doi.org/10.1007/s11135-017-0574-8 doi: 10.1007/s11135-017-0574-8
Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016, 2). Information security policy compliance model in organizations. *Computers amp; Security*, *56*, 70–82. Retrieved from http://dx.doi.org/10.1016/j.cose.2015.10.006 doi: 10.1016/j.cose.2015.10.006
Song, H., Fink, G., & Jeschke, S. (2017). *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications (IEEE Press)* (1st ed.). Wiley-IEEE Press.
Sophos. (2022, 4). *The State of Ransomware 2022* (Tech. Rep.). Retrieved from https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf
Stebbins, R. A. (2001). *Exploratory Research in the Social Sciences (Qualitative Research Methods)* (1st ed.). SAGE Publications, Inc.
Swinkels, R. (2017). *EU General Data Protection Regulation Compliance; Case study research focused on Dutch housing associations.* Tilburg University.
Tanriverdi, H., & Du, K. (2020, 12). Corporate Strategy Changes and Information Technology Control Effectiveness in Multibusiness Firms. *MIS Quarterly*, *44*(4), 1573–1617. Retrieved from http://dx.doi.org/10.25300/misq/2020/14223 doi: 10.25300/misq/2020/14223
Veiga, A. D., & Eloff, J. H. P. (2007, 10). An Information Security Governance Framework. *Information Systems Management*, *24*(4), 361–372. Retrieved from http://dx.doi.org/10.1080/10580530701586136 doi: 10.1080/10580530701586136
Verlaan. (2022, 4). *Woningcorporaties gehackt, ID-bewijzen en bankgegevens op straat.* RTL Nieuws. Retrieved from https://www.rtlnieuws.nl/tech/artikel/5299889/conti-ransomware-cybercriminelen-aanval-woningcorporaties
WerkenAanWonen. (2022, 3). *Onduidelijk hoeveel informatie de hackers bij deltawonen hebben buitgemaakt.* Retrieved from https://www.rtvoost.nl/nieuws/2080001/onduidelijk-hoeveel-informatie-de-hackers-bij-deltawonen-hebben-buitgemaakt
Westin, A. (1967, 6). Privacy and Freedom. *Washington and Lee Law Review*. Retrieved from https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/
World-Economic-Forum. (2022, 1). Global Risks Report 2022. Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
Yin, R. K. (2014). *Case Study Research* (5th ed.). Thousand Oaks, us: SAGE Publications.
Zakhour, Z., & Vasudevan, V. (2021, 11). *Atos predicts: The top 7 cybersecurity threats for 2022* (Tech. Rep.). Retrieved from https://pages.atos.net/rs/247-MBJ-716/images/atos_MARCOMThreat_Predictions_Paper_for_2022.pdf

Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010, 6). Information Security Risk Management Framework for the Cloud Computing Environments. *2010 10th IEEE International Conference on Computer and Information Technology*. Retrieved from http://dx.doi.org/10.1109/cit.2010.501 doi: 10.1109/cit.2010.501

Appendix

Appendix A - NIST framework - Functions and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 11
NIST Functions and Categories. Reprinted from 'Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework', by Brumfield et al., 2021, retrieved from https://ieeexplore.ieee.org/book/9820924: John Wiley & Sons, Inc., . Copyright 2022 by Cynthia Brumfield and Brian Haugli

Appendix B - Primary and supporting business processes - Overview

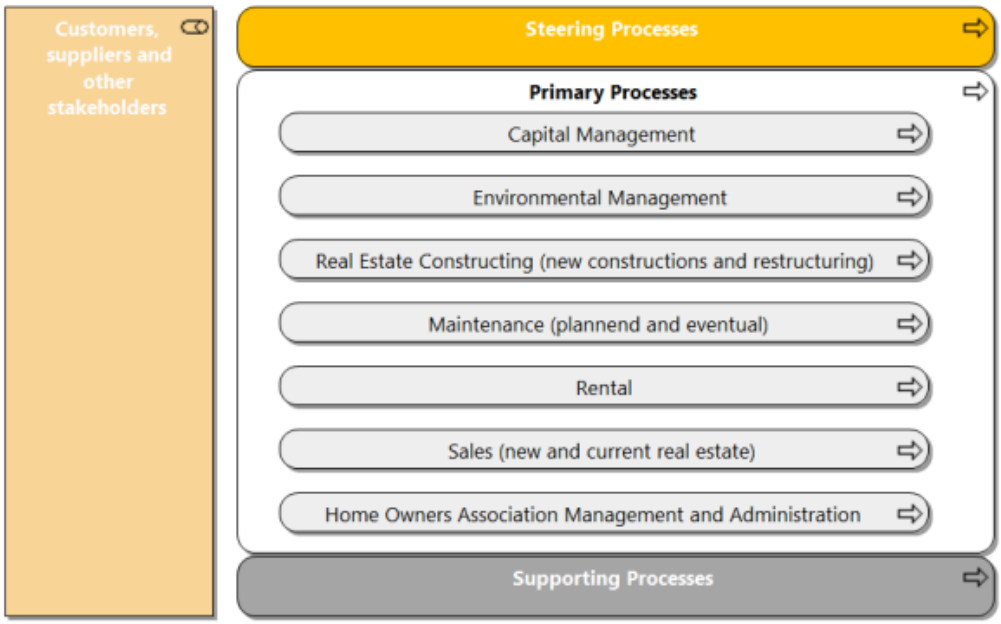

Figure 12
Primary business processes of Dutch Housing Associations. Reprinted from 'EU General Data Protection Regulation Compliance; Case study research focused on Dutch housing associations', by Swinkels (2017), retrieved from http://arno.uvt.nl/show.cgi?fid=144864

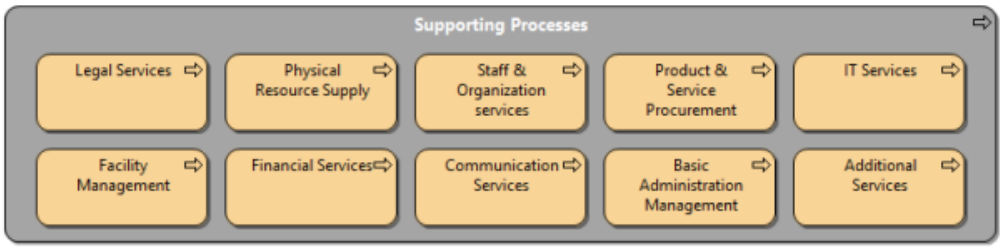

Figure 13
Supporting processes. Reprinted from 'EU General Data Protection Regulation Compliance; Case study research focused on Dutch housing associations', by Swinkels (2017), retrieved from http://arno.uvt.nl/show.cgi?fid=144864

Appendix C - Overview of participants

Number Name of organization	Name of participant	Function / Roles
E-1 Joanknecht	Lucas Vousten RA RE	Partner / IT Auditor & Advisor / Forensic Investigator
E-2 VVA-informatisering	Rick Swinkels Msc	Business Consultant / IT security & privacy specialist
E-3 VVA-informatisering	drs. Martijn Videler	Partner / IT security & privacy specialist
E-4 Xtract	Xander Koppelmans	Victim of a Cyber-hack and speaker on cyber-security conferences
E-5 Zig Websoftware	Olaf van Dijk	Director / Chief Information Security Officer (CISO)
C-1 Welbions	Lyn Besselink	Business Controller / Risk Management specialist
C-2 Wonen Zuid	Albert van Heugten MBI RI	Information Manager
C-3 Beveland Wonen	Sander Goudswaard	Information Policy Advisor / Security Officer
C-4 Alwel	John Dekkers MSc MBA	Business Controller
C-5 Stadlander	Henk Stoutjesdijk	Manager ICT / Security Officer / CISO

Table 3
Semi-structured interviews & Cases: Participants, Function / Roles, Organzations

Appendix D - Interview Guide - Case-Study interviews

Questionnaire for Housing Corporations:

- May I record the conversation?
- Do you agree if I mention your name and organization, as well as the outcomes of this interview in my research?

Your organization in general

1. What is your role in the organization?
2. Is your organization dependent on IT systems? Why?
3. Who is responsible for the following in your organization:
   (a) Cybersecurity (the protection of your digital systems against digital threats),
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks),
   (c) Privacy & information security (the availability, integrity, confidentiality, privacy and accountability of the information)
4. Is this one function or are there multiple roles assigned to a function? Why was this chosen?

Cyber threats and your organization

5. Has your organization been a victim of a cyber attack?
6. If yes, what kind of attack?
7. And what was the damage to your organization in terms of:
   (a) processes?
   (b) systems?
   (c) people?
   (d) finances?
8. Could you have prevented this attack? If yes, how?
9. What are the other lessons learned?
10. If you have not yet been a victim, is there a real threat of a cyber attack? Why?
11. Does your organization use cybersecurity frameworks (e.g., NIST, ISO 27001, ISO 27002)? If yes, which ones and why?
12. Does your organization have cybersecurity specialists on staff? Why?
13. Does your organization receive support in the area of cybersecurity? If yes, from whom? If not, does your organization need support? Why?
14. How does your organization currently stay up to date on current cyber threats? How could your organization stay even better informed about current cyber threats?

15. Does your organization work with other organizations in the area of cybersecurity?
16. Is your organization sufficiently secured against a cyber attack? Why or why not? What still needs to happen?

IT risk management and your organisation

17. Does your organization use a risk management standard (risk management standards, describe processes and are intended to identify and limit risks)? If yes, which one?

Context establishment

18. Is there a formalized (IT) risk management policy in your organization? And when does this date back to?
19. Are there subjects that are missing or receive less attention in your current policy?

Risk identification, Risk analysis, Risk Evaluation (Risk assessment).

20. How are cyber risks identified in your organization
21. How is the risk acceptance level (risk appetite) determined in your organization, and by whom?
22. How are risks classified, prioritized, and mitigated (processes to reduce the negative consequences of risks)? What measures have been taken or need to be taken? Are these measures structural? And sufficient?
23. How and with what frequency are risks within your organization evaluated?
24. How does a risk assessment take place within your organization?
25. What topics are missing or less common in your risk assessment and why?
26. Does your organization use a risk framework (such as ISO 27005, ISO 31000, COSO 2017)? And why or why not?
27. Are risks in your organization classified in a standardized way (chance * impact)?

Monitoring and reviewing

28. Are the risks evaluated and reviewed periodically? What is periodic?
29. Is the risk assessment methodology reviewed periodically?
30. How is the periodic performance of the IT risk analysis ensured?

Communication and consultation

31. In what form are the risks reported to management?
32. Is there an action plan / roadmap for mitigating identified risks in your organization?
33. Are IT risks sufficiently covered? Why or why not?

Privacy & information security within your organization

34. Does your organization use a privacy information security standard (ISO 27001, ISO 27002)? If so, which one
35. How is it ensured within your organization that information is always available (availability)?
36. How is the integrity of information ensured within your organization? In other words, how is the information protected against unauthorized or unusual modification or destruction?
37. How is it ensured within your organization that only authorized people have access to information? In other words, how is the information kept confidential?
38. How does your organization comply with privacy regulations? For example, by complying with the GDPR?
39. Are all actions in the different information systems controlled (auditability), and how is this done?
40. Are improvements needed in any of the above aspects? If so, which ones? Why?
41. Is the privacy and information security sufficiently safeguarded? Why or why not?

Appendix E - Interview Guide - Expert interviews

Questionnaire for Experts

- May I record the conversation?
- Do you agree if I mention your name and organization, as well as the outcomes of this interview in my research?

Your organisation in general

1. What is your position?
2. Are you also active in the housing association sector with your work? If so, do you consider housing associations to be heavily dependent on IT systems?
3. In your opinion, who should be responsible for:
   (a) Cybersecurity (securing your digital systems against digital threats)
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks)
   (c) Privacy & information security (ensuring the availability, integrity, confidentiality, privacy and auditability of information)
4. Do you often see this as one function or are there often multiple roles within a function? Why do you think this is chosen? How would you like to see it?

Cyber threats and your organisation

5. Victim of cyber attack?
6. Have you ever worked with a housing association that has been a victim of a cyber attack?
7. If so, what kind of attack?
8. And what has been the damage to the organization in question in terms of:
   (a) processes?
   (b) systems?
   (c) people?
   (d) finances?
9. Could this attack have been prevented? If so, how?
10. What are the other lessons learned?
11. If you have not yet experienced a victim, is there a real threat of a cyber attack in the housing association sector in your opinion? Why?

Cybersecurity

12. Do the housing associations you have worked with use cybersecurity frameworks (such as NIST, ISO 27001, ISO 27002)? If so, which ones and why? Do you think housing associations should work with these frameworks?

13. Do the housing associations you have worked with often have a cybersecurity specialist on staff? Why? If not, should they have a cybersecurity specialist on staff?
14. Do housing associations often receive support in the area of cybersecurity? If so, from whom? If not, do housing associations need support? Why?
15. How does your organization currently stay informed about current cyber threats? How could your organization stay even better informed about current cyber threats? How could housing associations stay informed about current cyber threats?
16. Does your organization work with housing associations on cybersecurity? Do you see many housing associations working together or seeking partnerships in the area of cybersecurity?
17. Are the housing associations you have been at sufficiently secure against a cyber attack? Why or why not? What still needs to happen?

IT risk management and your organization

18. Do the housing associations you have been at use a risk management standard (risk management norms, describe processes and are intended to identify and limit risks)? If so, which ones?

Context establishment

19. Is there a formalized (IT) risk management policy at the housing associations you have been at? And when does this date from?
20. Are there topics that are missing or less common in the policy and why?

Risk identification, Risk analysis, Risk Evaluation (Risk assessment)

21. How are IT risks identified in the housing associations you have been at?
22. How is the risk acceptance level (risk appetite) determined in housing associations, and by whom?
23. How are IT risks classified, prioritized, and mitigated (processes to reduce the negative consequences of risks)? What measures can be taken or need to be taken for this? And is enough being done within housing associations to properly regulate this?
24. How should risk assessments (assessment) take place within a housing association?
25. What topics are missing or less common in risk assessments and why?
26. Are risks in housing associations classified in a standardized way (chance * impact)? If not, should this be done?

Monitoring and reviewing

27. Are the risks at housing associations evaluated and reviewed on a periodic basis? What should be periodic?
28. Are the risk assessment methods evaluated periodically at housing associations? If not, should this be done? And how could this be done best?

29. How can the periodic execution of the IT risk analysis be best ensured?

Communication and consultation

30. In what form should the risks be best reported to management?
31. Do housing associations often have an action plan / roadmap for mitigating identified risks? How could this look best?
32. In your opinion, are the IT risks within housing associations sufficiently covered? Why or why not? What still needs to happen?

Privacy & information security within your organization

33. Are privacy & information security standards (ISO 27001, ISO 27002) currently being used in housing associations? If so, which ones? If not, would you recommend this?
34. How can housing associations ensure that information is always available (availability)? Is this already being done well?
35. How can the integrity of information within housing associations be properly ensured? In other words, how is the information protected against unauthorized or unusual modification or destruction? Is this already being done well
36. How can access to information be restricted to authorized persons within housing associations? In other words, how does the information remain confidential? Is this already being done well?
37. How do housing associations comply with laws and regulations regarding privacy? For example, through compliance with the GDPR? Is this already being done well
38. Are all actions within housing associations checked in the various information systems? (Auditability) and how is this done? Or how could this be done?
39. Are the information systems at housing associations regularly cleaned up? Irrelevant information removed?
40. In your opinion, are improvements needed in all of the above aspects? If so, which ones? Why?
41. Is privacy and information security adequately safeguarded within the housing association sector? Why or why not?

Appendix F - Information letter about research interview

Information letter about research interview: ***Cyber-vulnerabilities and IT risk management in the Dutch housing association sector***

What does participation in the research project involve?
You will be interviewed by me through a personal interview on location or through Microsoft Teams, if necessary. The interview will be a semi-structured interview and will last approximately 45 minutes. The interview will be recorded with your permission and transcribed afterwards so that I can use and find the information for the analysis part of my thesis. A smartphone will be used for the recording. In general, the interview will cover the following topics:

1. Your organization in general
2. Cyber threats and your organization
3. IT risk management and your organization
4. Privacy & information security within your organization

The main goal of the interview is to gain insights into how your organization currently deals with the various topics, namely cyber threats, IT risk management, privacy & information security. In addition, the goal is also to understand how your organization could potentially deal with the various topics in the future.

Is your participation confidential?
All information provided as part of the research will be treated confidentially. I will only provide your name or other information you provide to those for whom you have given permission. In the final research article, your name and information will only be used with your permission.

How is the information provided by you recorded, stored and protected?
After the interview, the recording is transcribed as soon as possible. The raw data is then immediately deleted. The information is securely stored on a laptop managed by me and in a Cloud environment as a backup. I will be careful to prevent loss of the data. The final transcript will be shared with you so that you can make any necessary changes. All interviews are held in Dutch but the final findings are written in English, it is also possible that quotes are written in English.

Participation in this research is entirely voluntary and you have the right to refuse participation. If you decide to participate, you also have the right to refuse to answer questions. In addition, you can withdraw from the research at any time without giving a reason. In the event that you withdraw from the research, you have the right to request that the data collected prior to withdrawal be deleted.

Who do you need to contact for more information?
If you would like more information, do not hesitate to contact me by email at T.IJpelaar@uvt.nl or by phone at +31 6 51895749.

Thank you in advance.

Sincerely,

Thomas IJpelaar

Under the guidance of Martijn Videler, Partner at VVA-Informatisering.

Appendix G - Codes

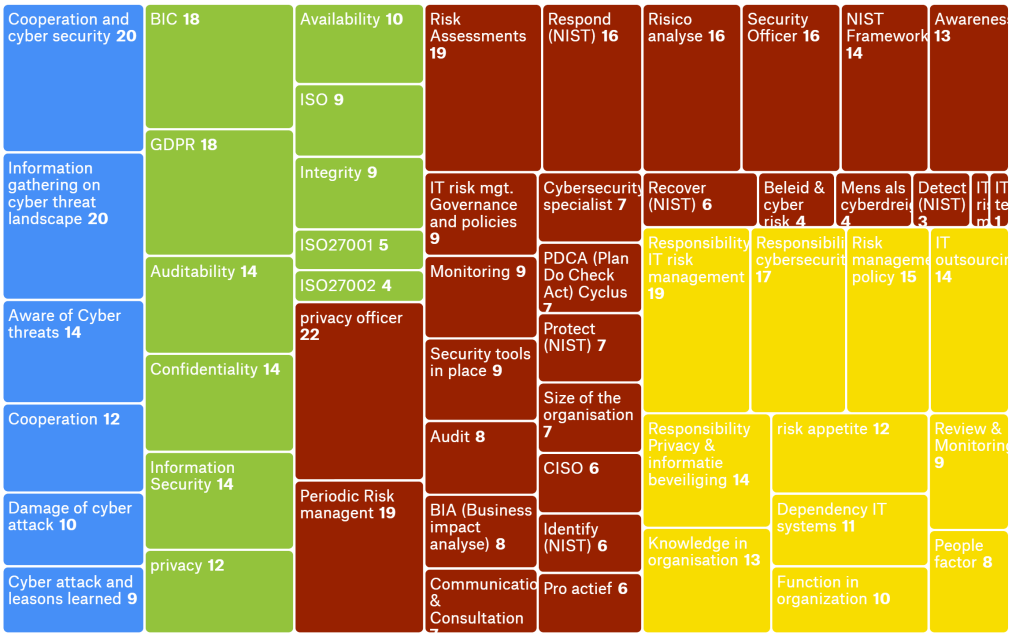

Figure 14
First-order codes and frequency

Appendix H - Case study interviews

Case study interview 1

Your organization in general

1. What is your role in the organization?

   I am an employee in the Control department at Welbions. Our team is responsible for risk management and internal audits, and also ensures compliance with regulatory requirements. We are also involved in projects, but not in their execution. Instead, we look at the legal requirements and risks for Welbions and provide warning signs and advice to complete the project as efficiently as possible. Privacy and information security are high on our list of priorities. For this reason, I am a member of the information security and privacy steering group, a kind of staff group. This is mainly due to the General Data Protection Regulation (GDPR) of 2018. We have looked for an organization that can help us guarantee privacy and information security. We have decided to form an expert group with representatives from HR, I&A or ICT, communication, processes, and myself. This choice is based on the requirements of the BIC. We have also included the manager of business operations as a liaison between the working group, management, and the board. This has worked well. However, like other housing associations, we do not have internal expertise for a privacy officer or security officer, so we have had these functions filled externally by our supplier Audittrail.

   Q: So Welbions obtaines knowledge regadering the privacy & security officers from an external partner?

   Yes, that is a competence, right? Or else we would have to have someone extra and have them go through a training.

2. Is your organization dependent on IT systems? Why?

   The scale of a housing associations determines how dependent they are on their system. Smaller housing associations often have a basic system, but are financially limited and may not always have the people with the right specialization to digitalize the entire system. If there are many older people working at a housing association, this can also affect the dependence on digitalization. However, this does not apply to all housing associations.

   Q: So if the IT systems stop functioning, the work can continue?

   Whether a housing association needs an incasso application depends on the size of the association and how they have set up their processes. For example, at a small association with 1000 tenants, a financial package can send a payment reminder if a manual approach is sufficient. But at large associations, this may be different. Housing associations must also take into account the wishes of their customers, including the desire for digitalization among young people. For example, in our association, we have many one-person households with a young age who always have a phone with them and can easily find a customer portal.

3. Who is responsible for the following in your organization:
   (a) Cybersecurity (the protection of your digital systems against digital threats),
   It is the responsibility of everyone to implement technical security, but the human is always the weak link in cybersecurity. That is why it is a subject that is not only for management, but for everyone. This is also the challenge for housing associations if they are highly dependent on digitalization. Cybersecurity is very important in this world. Although the board is ultimately responsible for addressing cybersecurity, everyone should feel responsible for it and be aware of its importance.
   Q: So the responsibility should be felt troughout the entire organization?
   Yes, if someone says no, I don't want to be responsible for that. Then we have a problem immediately.
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks),
   Managing IT is a collaboration between different aspects, such as technology and policy. Within a company, there are frameworks needed for IT management to determine the choices the company makes, such as taking out a ransomware insurance policy. Risk management is not only the responsibility of the board, but also of every employee who needs to recognize responsibilities and not just exercise rights, but also bear the burdens. This applies, for example, to the use of laptops, for which policy is needed to manage the risk. Policy is also needed for teleworking and it is important that employees are well informed. Within Welbions, the IA department is responsible for part of the IT risk management, such as password management and backup, while the Control department is responsible for the strategic side, such as reporting on information security as a risk.
   (c) Privacy & information security (the availability, integrity, confidentiality, privacy and accountability of the information)
   First you have the legal environment, for which you need a privacy or security officer. For all three of the questions you ask, about the three topics, it is important that the entire company takes part in the responsibilities.

4. Is this one function or are there multiple roles assigned to a function? Why was this chosen?

   Assigned to different people. Some organizations just have very few people. Organizations look at the people and their competence and then say, we don't have it in-house, then it can be obtained externally.

   Cyber threats and your organization

5. Has your organization been a victim of a cyber attack?

   No

6. If you have not yet been a victim, is there a real threat of a cyber attack? Why?

Recently, we have heard a lot of rumors about ransomware cyber attacks. It remains a threat that we must be alert for. Every housing association must realize that they are also vulnerable. We have looked at insurance policies, but only 25% of the sector is involved with this. We have a lot of sensitive tenant information in-house. Therefore, we must see it as a real threat and deal with it well.

7. Does your organization use cybersecurity frameworks (e.g., NIST, ISO 27001, ISO 27002)? If yes, which ones and why?

   The Baseline Information Security (BIC) is a standard to which risks and key performance indicators (KPI's) are linked. Although it is not mandatory, it is recommended to comply with it. We have carried out a baseline measurement to determine what needs to be done to comply with the BIC. The BIC promotes awareness and helps to tick off what has been done to meet the standard. The BIC is the framework within which we work

   Q: Why is the BIC used often?

   Housing association specific. We are a party between the government and commercial. Housing association also have laws and regulations

8. Does your organization have cybersecurity specialists on staff? Why? Or does your organization receive support in the area of cybersecurity?

   At Welbions, we have hired a security officer to help us monitor our cybersecurity. We already have an I&A coordinator, but so much is happening and we also want to be aware of what is going on. For example, we want to know which applications are in the risk group. In addition, it is also important that we have good communication with our suppliers, such as our network administrator 'Previder', where we have our servers managed. This is not only important for our cybersecurity specialist, for our security officer, but also for the specialists on the supplier side. For this, we need good communication channels.

   Q: So indeed a good communication channel needed to get that support in the area of cybersecurity, but also to see if the yes where you outsourced it to your network administrator actually has everything in order?

   Yes.

9. How does your organization currently stay up to date on current cyber threats? How could your organization stay even better informed about current cyber threats?

   Currently, we have about 40 applications within and outside our primary system, both in the Cloud and with various suppliers. It is complicated to keep track of all events and if a supplier is hacked, we are also immediately next in line. That is why it is important to plan business continuity. We started with this this year and we already see the risks we have. For example, we need to classify our information to know which information is sensitive and to continue if a supplier is hacked. My opinion is that it is not always possible to be aware, but we must have a business continuity plan in-house and know who is responsible if

something fails. We must also have a cyber incident response plan and good communication lines with our suppliers, not only to meet the SLA, but to become part of a cycle where we keep each other informed of developments within the company. After all, we have many relationships and cannot be aware of everything. Internally, the plans must be ready in case something is wrong.

10. Does your organization work with other organizations in the area of cybersecurity?

    At the moment, not yet.

    Q: Do you see an opportunity in this in the future?

    Working with housing associations can bring benefits in terms of Economies of Scale. By working together, we can use shared experience and prioritize risks together. Cooperation is important not only for cybersecurity, but also in other areas. My opinion is that cooperation between housing associations is not being used enough, because too much emphasis is placed on the idea of "my territory" and "my tenants". This is a pity, because we can learn a lot from each other and also save money. There are certainly opportunities to act together when there are problems.

11. Is your organization sufficiently secured against a cyber attack? Why or why not? What still needs to happen?

    It's not possible, right? I mean, even the best companies get hacked, so you can never really be sufficiently prepared. That being said, we do need to try to protect our critical processes with critical information and all our crown jewels.

    Q: Do you think housing associations often have insight into what those crown jewels are?

    That's what I'm saying with the business continuity plan. It starts with the business impact analysis, where we look at each process and ask, what are our critical processes? I don't know if many housing associations already have such a plan, but we don't yet. We always need to be alert to security and that's what we're talking about now.

12. Does your organization use a risk management standard (risk management standards, describe processes and are intended to identify and limit risks)? If yes, which one?

    IT risk management is a key aspect of our operations at Welbions. We use the BIC and external accountants who have a standard for analyzing risk management and housing associations. At a strategic level, we also have a risk map that we review and discuss annually with employees, managers, the board of directors, and the board of commissioners. Measures are established to minimize risks and prioritize priorities. IT risk management within housing associations is often formalized and is approved annually by the board of commissioners. Unlike commercial companies, such as listed companies that often use COSO, at Welbions we have a risk management policy that includes IT risk management.

13. Is there a formalized (IT) risk management policy in your organization? And when does this date back to?

    Well, we do have one. We have a policy that is discussed and approved by the Board of Directors each year.

14. Are there subjects that are missing or receive less attention in your current policy?

    Management has had information management and data management on the agenda for three years. This year, we have specifically focused on information security, which is high on the agenda.

15. How are cyber risks identified in your organization?

    No, we have that from the BIC. We have all the risks of the Information Security and Privacy Steering Group. Each year we create an action plan based on the annual assessment of privacy and information security. That assessment is also based on the BIC. Every time we do a gap analysis, we identify the risks. In addition, we also have interim control from accountants. We look at things like whether change management is sufficient. Sometimes risks arise from within the organization, for example if we receive signals that the Clean Desk Policy is not being followed. This comes from various sources.

16. How is the risk acceptance level (risk appetite) determined in your organization, and by whom?

    There are various factors that play a role in determining the risks a company takes. For example, it depends on the company itself and the industry it operates in. For us as a housing association, there are specific rules we have to follow, such as the Housing Corporation Authority and certain financial ratios. There are also things like market values that play a role. When it comes to cyber risks, it is important to consider the potential consequences of these risks and decide whether or not we want to take the risk. For example, by investigating a ransomware insurance. Security is also an important aspect that we always have to take into account. When it comes to risks in general, it is important to carefully consider the potential consequences of a particular decision and decide whether or not we want to take the risk.

17. How are risks classified, prioritized, and mitigated (processes to reduce the negative consequences of risks)? What measures have been taken or need to be taken? Are these measures structural? And sufficient?

    It is difficult to determine which measures are best to take to mitigate risks. It depends on the specific context of the organization, such as the size of the company, the way the process works, and the people who work there. Awareness of the importance of security is obviously important, but it is also important to invest in technical measures such as periodic penetration tests and data protection impact analyses. It is difficult to say what is specifically important for an organization, so it might be helpful to ask specific questions about the processes and technology and to see which measures best fit your needs.

18. How and with what frequency are risks within your organization evaluated?

    I understand that you are asking about the importance of continuous monitoring. If it is important, I will certainly mention it. I just want continuous monitoring. I'm wondering what you think is important and what is less important. It would be better if this question is formulated in a clear way so that we can get a better picture. For example, we at [housing association] make reports every 4 months about the most important activities in the risk map. This depends on the activities we carry out. If, for example, a new project is started, we can monitor it to see how it is being carried out.

19. How does a risk assessment take place within your organization?

    It is difficult to answer your question without more context. It appears that you are talking about risk assessment and it depends on how the company is. If you are talking about this year, you do something different next year. You depend on how you want it to be.

    Q: And how would you like it to be?

    It is important to know what risks you have before you can assess them, because it is difficult to assess if you do not know which risks are high or low. I wonder what measures you should take and whether you should do it immediately or whether you can wait. It is also important to know how much you need to invest. It depends on the situation and the risk you have. It is useful to divide it into small groups with their own risk capital and the type of risks they have. Some corporations are further along in digitization than others.

20. What topics are missing or less common in your risk assessment and why?

    That's a difficult question, I'm not able to provide a good answer for that.

21. Are risks in your organization classified in a standardized way (chance * impact)?

    Our standard for assessing risks is to use a high, medium, low approach, which means we do a risk and impact analysis through discussions with stakeholders. We also use colors to indicate the level of risk - red means high, green means low. However, it is important to remember that this is not static and that the risk can change over time. We must therefore continue to monitor and regularly update the risk analysis.

22. Are the risks evaluated and reviewed periodically? What is periodic?

    We do a monitor every 4 months to see what is happening. When preparing the report, we have to ask everyone what has happened. I think continuous monitoring is important because otherwise the risk awareness is lost if you just tick boxes and make reports. Active monitoring is also important because it is not just about making reports, but also about taking action based on the risks we see. For example, if we see a high rent loss in a certain area, what can we do to reduce it? Some housing associations are very active in this, for example by using platforms such as Aedes

Communities where they can share what is happening with them and what they think about it. Sharing information about cyber attacks in these types of groups should happen more often. Not only in the IA department but everyone should be aware. This is also a form of active monitoring of risks because it increases awareness and enables people to take action.

It often happens annually, but sometimes later, that the risks a corporation faces are looked at. This depends on how the corporation assesses the risks. There are standard risks, such as legislation, that cannot be avoided. That is why it is important to continuously monitor these so that we are aware of any changes. In addition, there are also strategic risks, such as sustainability, which require a lot of legislation. With us, financial risks are particularly closely monitored, using a specific application we have purchased for this purpose. This is important because it costs a lot of money and is also important for the tenants. Monitoring of risks can take place at different levels, depending on how the risks are seen. Sometimes we invest in real-time monitoring, for example for the sustainability of a complex.

23. How is the periodic performance of the IT risk analysis ensured?

The conclusion is that it is important to be proactive in carrying out periodic analyses or checks, because if you are too late, it is not worthwhile to carry them out. It is also important to be aware of what is happening in the world, because then you can also look at the vulnerability of your suppliers. For example, if a kitchen specialist is hacked, this can lead to supply problems and impact our program and ultimately also our tenants. So it is not only important to focus on the vulnerability of our own company, but also on that of our suppliers.

24. In what form are the risks reported to management?

Management always wants something official. If I look at our company, it is also important to have reports that can be scanned and stored on laptops. But what is more important are agreements and taking responsibility. So a report should not only be a report, but also a task agreement. As a manager, you are responsible for carrying out risk analyses. In some companies, like ours in Twente, it can be difficult to address each other and maintain peace, but sometimes it is necessary to change the culture in order to effectively work on risk management. The culture of a company can also influence how people deal with risk management. Sometimes people will say it is not their responsibility, while in other companies people are proactive and address each other on their responsibilities. It is important to consider the company culture when determining how to best approach risk management.

25. Does your organization use a privacy information security standard (ISO 27001, ISO 27002)? If so, which one?

Do you know the Corponet website? There is a lot of information to be found there about risk management for housing associations. They have also done research on the city of Zuid. I think it would also be interesting

to get more background information. In addition, Corporatie.nl does a lot of research in the area of information security for housing associations.

26. How is it ensured within your organization that information is always available (availability)?

    I find this a strange way of posing the question. Because we are now looking at privacy and information security

27. How is the integrity of information ensured within your organization? In other words, how is the information protected against unauthorized or unusual modification or destruction?

    To give you an idea, I have around 14,000 housing units. When I say that the quality of these units is compromised, I mean that they are modified or destroyed. This may be in violation of the GDPR (General Data Protection Regulation), which requires us to safeguard the integrity of data in test environments and anonymize it. When I say that someone can mutate the units, it means that they can change the structure, but these changes are only visible within the organization. So it's not that I can only mitigate, but it is difficult to guarantee the safeguards. In an ideal situation, I would be able to determine who is responsible for each change to a unit. If we carry out a process, someone can do certain things that can be translated into other processes, so that I know exactly how each process was carried out. It is important to safeguard the integrity of data through good organization of the lines of control, such as a second line and an accountant. Although it is not possible to guarantee the integrity of data at 100%, there are moments in the planning and control cycle when we try our best to achieve this. There are also moments in the organization when the integrity of data is not properly handled.

28. How is it ensured within your organization that only authorized people have access to information? In other words, how is the information kept confidential?

    Within an organization, the authorization process is important to determine who has what rights to perform certain tasks. It is important to organize this process well, so that everything is clear and there is no confusion. For example, when new employees join, it is necessary to set up a chain for requesting, granting, and checking rights. This can be done through a separate authorization module, but it also depends on the specific needs and structure of the organization. To ensure that the authorization process continues to work efficiently and effectively, it is advisable to carry out regular checks. How often these checks take place depends on how the structure is set up and how much trust there is in this structure. For example, if the structure is considered good, it may be sufficient to carry out checks twice a year. Some organizations also have real-time reports that allow them to see who has what rights and what they are allowed to do.

29. How does your organization comply with privacy regulations?

    I agree that the fines and such from housing associations make sure that the information security is actually very basic. That's actually good,

because privacy is important. It has nothing to do with us as individuals. In the first year we were forced to do this, but now we see that it is important to do this for each other, given the circumstances.

30. Are all actions in the different information systems controlled (auditability), and how is this done?

    Within a housing association, it is important to manage information systems well. There are different types of information systems, such as applications that process personal data and financial packages. For applications that process personal data, it is important to set up a processing agreement. This agreement sets out the conditions that apply to the processor of the personal data. An audit of the processor can also be included as a condition in the processing agreement. However, for financial packages, it does not seem necessary to carry out an audit. It is important to make a distinction between these different types of information systems, as this determines which rules and conditions apply.

31. Is sensitive privacy information regularly cleaned up at housing associations?

    This is a good question. I understand that it is important to efficiently store and manage documents and information. This is made necessary by the GDPR obligations to observe retention periods and the volume of information you process. It is also difficult because the retention periods depend on the type of information and the management system you use. For example, it is easier to store financial data than information on livability, because the latter takes much more time to assess and store. You try to deal with this challenge efficiently, for example by using a smart file management system, but this proves difficult because there is not always enough time and investment put into setting up an efficient system. It is also difficult because you sometimes depend on the technology you use. If you store all information in a common folder, it can be kept for 100 years, but it is difficult to quickly and easily access specific documents. It is therefore important to look for ways to address this challenge and efficiently manage information management.

32. Is the privacy and information security sufficiently safeguarded? Why or why not?

    No, of course not. Otherwise, I would never have this conversation. Yes, as I said, even the best companies can be hacked

Case study interview 2

Your organization in general

1. What is your role in the organization?

   Within the management team at Wonen Zuid, I am responsible for information provision and automation (I&A). That includes both analog and digital systems for providing information. I lead a team of four departments, including the department for general affairs with a coordinator for projects. A department for documentary information provision. A department for IT and a department for Business Intelligence. My specific role is to focus more on information management. This means that I am also responsible for drafting the long-term strategy for the further development of our information house, including IT sourcing, information security, and the protection of personal data according to the GDPR. The roles of privacy officer and security officer are filled from my team.

   Q: Can you tell me something more about Wonen Zuid?

   Wonen Zuid is a housing association with an area of operation in central and southern Limburg. We own 14,000 homes and an additional 2,000 units, such as garages, parking spaces, social housing, and retail spaces. We employ approximately 170 people, although not everyone works full-time.

2. Is your organization dependent on IT systems? Why?

   Yes, very dependent. The degree of automation and digitization in this organization is such that we are very dependent. This organization is so dependent on systems that you can't do anything if a malfunction occurs. It's important to be well prepared for potential issues with the systems.

3. Who is responsible for the following in your organization:
   (a) Cybersecurity (the protection of your digital systems against digital threats),
   The board. But this is a task that has been delegated from the board to me as a manager. Within my team, we have two officials who are responsible for protecting personal data as the privacy officer under the GDPR. And an employee who is responsible for information security, the security officer. When it comes to the code for information security or the Baseline Informatiebeveiliging Coöperaties (BIC), they are responsible for compliance with these guidelines.
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks),
   The responsibility lies with the management. Together with the Control department, I play a role in implementing risk management, and I am involved in identifying risks. The control team's task is to give advice to the management on risk readiness. My team then has the responsibility to mitigate risks, but we don't determine the policy. Our role is to identify risks and the risk readiness is up to the management. Mitigating undesirable risks is

the responsibility of my team. The team is clear about our roles and responsibilities.

(c) Privacy & information security (the availability, integrity, confidentiality, privacy and accountability of the information)
The official within our team who fulfills the role of privacy officer, also chairs a working group for the General Data Protection Regulation (GDPR). This working group regularly keeps a finger on the pulse to ensure that we continue to comply with the GDPR. If there are privacy incidents or if someone, such as a tenant or an employee, wishes to exercise the right to be forgotten or the right of access, the privacy officer takes action. They then review the file and determine how it should be further handled.

4. Is this one function or are there multiple roles assigned to a function? Why was this chosen?

   The GDPR (General Data Protection Regulation) came into effect on May 25, 2018. At that time, there was no specific place or organization within Wonen Zuid where this was well established. In January 2019, Wonen Zuid carried out a reorganization, in which the Team Informatization and Automation was renamed as information provision and automation and added the analog world too. I was also made responsible for documentary information provision, and since then I have also been responsible for the GDPR, the protection of personal data and overall information security. I have then stated that the roles of security officer and privacy officer are needed. Two separate people have been appointed for privacy and security, as these are two different things.

   In the discussion and conversation, it may occur that the different positions and perspectives are sometimes contradictory, despite the great overlaps. However, it is important that these functions have each other as a sounding board. In my role, I have mainly focused on the technical aspect of information security. If you look at the theories, information security is about the availability, integrity, and confidentiality of information. This is supported by three pillars: the human, the organization, and the technology. Before January 1, 2019, we had mainly focused on the technology, but since then we also focus on the organization and the human. This means that my team will work both the privacy officer and the security officer with the policy paragraph. Information security, also the ISMS from ISO27001, also the PDCA (Plan Do Check Act) Cycle that must be completed annually to ensure the control of the system. Within my team, we make assessments based on the management measures from ISO 27002. We also help the control department and management to protect our most important assets (crown jewels) and to gain insight into our risks. If we look at the side of the GDPR, this was initially an ad-hoc function. Only after the data protection law transitioned to the GDPR, did this function receive a real position in our organization.

   Q: Is it currently well-organized and in order? Or is there room for improvement?

To assess the quality of our information security, we regularly carry out assessments and engage in benchmarking. We also perform tests such as Pen tests, phishing tests, and social engineering. Although we do well in these, it is never completely good enough. As cooperatives, we currently carry a great risk with us, as even clicking on a wrong link can put us all in danger. This means that we need to be aware of our behavior and ensure that we have recovery plans and a business continuity plan in place, with time schedules and priorities for restoring our systems.

Cyber threats and your organization

5. Has your organization been a victim of a cyber attack?

   Define a victim. Have we gone down?

   Q: Yes, whether or not you have gone down.

   Have we ever been hit by cyber attacks? No. But have we dealt with cyber threats? Yes, recently we experienced a severe attack where we had to deploy additional monitoring for several weeks to protect ourselves. This cost us hundreds of extra hours, but fortunately we managed to stay unscathed.

6. Is there a real threat of a cyber attack? Why?

   Cyber threats are a real risk and occur every day. By monitoring our system and looking at our firewalls, we see daily attempts of attacks. Some are insignificant, but sometimes they are very serious and require additional measures. It is important to always be vigilant and take measures to protect ourselves against these threats.

7. Does your organization use cybersecurity frameworks (e.g., NIST, ISO 27001, ISO 27002)? If yes, which ones and why?

   An article was published today in the Corporate Guide about the new generation BIC that is currently being built. I am the lead author of the BIC. I have been working in the housing corporation sector since 1983 and have been active in IT since 1990. Since 2000, I have been responsible for the management of IT and automation. We have always run our own data center services until 2019, but from 2020 we have outsourced the entire technical management and entire technical operations, while we have taken on a heavy oversight role in relation to our supplier, in the field of cyber. In the 25 to 26 years that we have been active in Wonen Zuid with the internet, we have never been successfully hacked so far, although we are confronted with attempts every day.

   Q: So you are using the BIC, are there other frameworks that are also used?

   When we look at frameworks, at Wonen Zuid we are looking closely at the ISO 27,000 series, specifically 27.001 and 27.002. We use this to define our risk profile and measures to mitigate them. We also look at other versions of these standards, in which the BIC 4 also plays a role and anticipate developments such as chain automation, outsourcing and SaaS. In fact, we are looking at the code for information security from a broad perspective.

In the latest version of the BIC, the fourth generation BIC from 2022, we apply the latest standards and norms prescribed in the directive.

8. Does your organization have cybersecurity specialists on staff? Why?

   Yes, the security officer that Wonen Zuid employs is a cyber security specialist.

   Q: And why was this person hired?

   To ensure that we can keep our information in-house available for the organization and to prevent us from getting infected with viruses or ransomware, we need to safeguard our business continuity. This means that we need to be aware of the key aspects of information security: availability, integrity and confidentiality. If we don't know where the threats come from, we run the risk of getting affected.

9. Does your organization receive support in the area of cybersecurity? If yes, from whom? If not, does your organization need support? Why?

   That is twofold. Wonen Zuid has an infrastructure partner for technology, Claranet with a Secure Competent Center (SOC). We have regular meetings with Claranet on the technical aspects of information security. Additionally, we use different tools to improve awareness within our organization, on the human side. We do this through an awareness campaign, periodic cyber security conversations with teams and phishing tests. We also use KPN Security, a third party, to regularly have us externally evaluated. This allows us to see how resilient we are.

10. How does your organization currently stay up to date on current cyber threats? How could your organization stay even better informed about current cyber threats?

    That has a lot to do with the fact that the security officer, the privacy officer, and myself are very closely monitoring certain things. We keep ourselves informed about threats in the sector by checking the websites of reputable parties, such as McAfee and Checkpoint. We also follow websites of DTC (digital trust center), NCSC to stay updated on what is happening in the world. With colleagues from the housing corporation sector, I am currently working on setting up a housing corporation-specific ISAC (Information sharing and analysis center), so that we can have an alarm system within the sector.

11. Does your organization work with other organizations in the area of cybersecurity?

    Sharing knowledge about information security is becoming increasingly important. We are affiliated with the special interest group cyber security at corponet, where cooperatives share information with each other to keep each other informed of threats. We do a lot together, but this mainly revolves around signaling to each other.

    Q: Keeping each other informed?

    Yes. About that WoCo ISAC, it will be released to the sector next week.

12. Is your organization sufficiently secured against a cyber attack? Why or why not? What still needs to happen?

    What is enough? I can't say yes to that.

    Q: What still needs to be done in this field?

    Always. It's important to remain vigilant and to continue working to improve information security. It's also important to keep learning and staying up to date on the latest developments and threats in the world of cyber security. It's also good to work with other organizations and share what you know and learn, so that everyone can benefit from collective knowledge and experience. It's also important to have good policies and processes and to continue improving them, so that you can deal with cyber risks in a structured way and manage them. My role is to continuously seek a balance between providing a functional system to the organization and preventing unnecessary obstacles. It needs to be functional, so people can easily access the system, but at the same time it's also important to know who comes in and who doesn't. Also because every day there's huge outflow of personnel and often there are also changes of function. Additionally, we also have to account for risks of internal people making mistakes. Although cyber risks are an important topic, we also need to consider internal risks.

    Q: Yes, the human factor also applies there?

    It's not just about the human factor in the sense of people being aware of risks, but people can also be malicious. It's also important to prevent people from being tempted to do wrong things within the organization, such as trying to hack the HRM system or steal customer data such as IBAN numbers and balances. This can be just as damaging as external cyber risks. It's important to have a good firewall to protect the organization from these types of risks. And what is considered secure? There are different ways to enhance the security of an email environment, such as using security protocols like Transport Layer Security (TLS). This is a protocol used to enhance the security of internet communication, such as sending emails. Additionally, tools such as firewalls and antivirus software can also be used to increase the security of an email environment. As I mentioned earlier, it's about finding a balance between a low barrier of access so that people can easily access the system, but also being aware of what is coming in and what isn't. When is it okay? When is it not okay? Who is okay, who is not okay?

IT risk management and your organisation

13. Is there a formalized (IT) risk management policy in your organization? And when does this date back to?

    Wonen Zuid's formalized risk management policy was implemented in the first quarter of 2022, and is currently scheduled for review in the first quarter of 2023. The policy is less than a year old and is already on the agenda to be revised.

14. How is the risk acceptance level (risk appetite) determined in your organization, and by whom?

    Whereby the board and management determine how much risk they are willing to take. On the other hand, it is also important to look at your own responsibility and work from the principle of "zero trust". This means that you assume that no one can be trusted automatically and that all access to systems and information must be controlled. This can be done by means of security measures such as implementing the SIS (Secure Information Sharing) manual.

15. How and with what frequency are risks within your organization evaluated?

    We took two years to fully go through the PDCA cycle in the context of ISO 27001 and ISMS. The ambition is to do it annually.

    Q: And why annually?

    That's also because Wonen Zuid is willing to invest more hours into it.

16. Are risks in your organization classified in a standardized way (chance * impact)?

    Yes, we use a risk management tool called 'Fully in Control.' Our team uses this framework for control and governance. Within that, there is also a classification methodology. We indicate which risks we have and what we can do to mitigate them. Our Concern Control department consults with us on the framework for risk readiness, where we apply the zero trust principle at the front end. This means that Concern Control will not easily say that something is not good enough.

17. Is the risk assessment methodology reviewed periodically?

    I can't say for sure. We have been using the control system for a few years. As I told you earlier, we filled out the entire model for the first quarter of 2022, including IT risks. Now, at the beginning of the first quarter of the next year, we are ready for another iteration with an annual frequency. So yes, annually.

18. In what form are the risks reported to management?

    Extracts are made from the tool based on reports supported by 'Fully in Control.' The concern Control also discusses the risk profiles with the management, and specifically with me as the security officer and my manager.

19. Is there an action plan / roadmap for mitigating identified risks in your organization?

    When you look at the Plan Do Check Act (PDCA) model, this means that when you identify your risks, you will take certain actions to improve security. We also have an action item list that we work on together with our vendor, particularly in a technical area. Additionally, we keep track of our policy and PDCA on an annual basis, and continue to create awareness by using tools on a bi-weekly basis.

Q: What does that look like on a bi-weekly basis?

We have an app that conducts a chat dialogue on cyber risks and GDPR risks with colleagues.

20. Are IT risks sufficiently covered? Why or why not?

When you look at the penetration tests that KPN Security conducts with us on a regular basis, we have a clean slate. When we first had a penetration test done, a few things were identified. We solved those. We also test regularly again to ensure our slate stays clean. We also regularly have external evaluations, and if you look at COBIT, you have certain maturity classes from 1 to 5. Wonen Zuid wants to achieve a high score. We recently had an audit done by an organization that does many assessments worldwide and also nationally in this area. Our score was better than the sector average in the Netherlands, so we have a good score."

21. How is it ensured within your organization that information is always available (availability)?

I do my best to ensure security, but I cannot guarantee that there is no one who can take us down. However, I do more than a justifiable, utmost effort to make sure everything stays safe.

22. How is the integrity of information ensured within your organization? In other words, how is the information protected against unauthorized or unusual modification or destruction?

Yes and no. If you look at transaction-processing systems, such as an ERP, then there are all kinds of programmed controllers and plausibility controls that ensure that no strange things can happen (so-called soft controls). In addition, we have tight authorization schemes, in which the access rights of a role-based profile are precisely determined for each function. This means that each function has specific limits for, for example, task assignment or invoice approval.

23. How is it ensured within your organization that only authorized people have access to information? In other words, how is the information kept confidential?

If a system is well secured, you only have access to what is based on your role. We use the RBAC (role-based access control) mechanism here. This means that at the front we already check whether an employee may have access to a certain environment. Within this environment, it is again regulated what an employee may do and to what extent they may do something. This is very precisely worked out for all employees, applications, roles, and cross-references between these elements.

24. How does your organization comply with privacy regulations? For example, by complying with the GDPR?

We closely follow the guidelines of the GDPR and have no reason to adjust our policy plans. We comply with these guidelines. If legislative changes are implemented or announced, the GDPR working group (consisting of the privacy officer and the company lawyer) will consider what this means

for us and there may be a need for a change in our privacy policy, such as in procedural matters, disaster plans or reporting to the Dutch Data Protection Authority (DPA).

25. Are all actions in the different information systems controlled (auditability), and how is this done?

    Not all, but the most relevant ones. We have audit trails running on critical places on different systems.

26. Is information that is no longer needed in the organization also removed from the information systems?

    In the context of the GDPR, we have established a retention and destruction policy, in which the retention obligations and destruction deadlines are indicated for each type of information. We also carry out periodic cleanup in our organization and use technology, such as AI, to remove unwanted records. For example, if we accidentally register a BSN number in our CRM system during a conversation, we use AI to remove it.

27. Are improvements needed in any of the above aspects? If so, which ones? Why?

    That is a question of conscience, when is it not? I believe that in my role and responsibility, I am in control and do everything that is expected or required of me and have it in the pocket. But that does not mean that I should not stay alert and aware of any threats. I will continue to proactively mitigate instead of coming after the fact.

28. Is the privacy and information security sufficiently safeguarded? Why or why not?

    We give ourselves a passing grade, but it remains a permanent challenge to ensure it stays that way. But we must always remain alert and prepared for possible threats. If we are faced with a severe attack where we are severely compromised, we have our playbooks ready.

Case study interview 3

Your organization in general

1. What is your role in the organization?

   I'm I&A policy advisor and security officer at Beveland Wonen.

   Q: What kind of organization is Beveland Wonen?

   We have about 125 employees and they are divided into different departments and my position falls under the Director of Housing. It falls within the Organization and Development Department and I am an I&A policy advisor. But I am not part of the I&A department and I can independently advise both I&A and the board.

   Q: And how many tentants do you have at Beveland Wonen?

   Approximately 11.000.

2. Is your organization dependent on IT systems? Why?

   Without IT you no longer have an organization.

   Q: Why? How do you mean?

   All important business processes are dependent on IT. The most important component is the ERP system, in which everything related to real estate is recorded and processed. If that system is not available then you can not perform most processes. Because they are all linked in some way to that system. So indeed very strongly dependent on the IT systems.

3. Who is responsible for the following in your organization:
   (a) Cybersecurity (the protection of your digital systems against digital threats),
   That function is assigned to me as a security officer and of course I am not ultimately responsible. But I am responsible for the content of security, which is both the hard and the soft side of securing
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks),
   Our Control department.
   (c) Privacy & information security (the availability, integrity, confidentiality, privacy and accountability of the information)
   We have a privacy officer for that, they are responsible for that. The part of information security that falls under me, under security.

4. Is this one function or are there multiple roles assigned to a function? Why was this chosen?

   I have been working at this organization for less than a year, so this structure that was devised before I worked here.

   Cyber threats and your organization

5. If you have not yet been a victim, is there a real threat of a cyber attack? Why?

That threat is very real because we see among our colleagues that they have already become victims in large or small ways. And we also see very regularly that attempts are made by means of phishing for example.

6. Does your organization use cybersecurity frameworks (e.g., NIST, ISO 27001, ISO 27002)? If yes, which ones and why?

   Our information security policy is based on the BIC 3.0 at the moment. Version 4.0 is in development and is expected to be released next year. The BIC is based on the ISO 27.001 standard and is more specifically tailored for the housing association world.

   Q: What makes the BIC specifically made for the housing association sector?

   The difference between the ISO and the BIC is that the ISO dictates a massive set of guidelines without specifying them in more detail, whereas the BIC provides a baseline. So it says you should at least have this regulated. This is very different from the complete spectrum from which you have to choose what to do and to what extent. We are working with the NIST framework and we expect to make further progress in it next year. We also want to work with "Fully in Control", a risk management system that allows you to work structuredly with all these standards.

   Why did your organization add the NIST?

   Because NIST has a different approach and yes, NIST is based on 5 pillars, as you may also know. By working from these five pillars, you can look at your landscape much more focused and see which measures you want to take.

7. Does your organization have cybersecurity specialists on staff? Why?

   Yes, me.

8. Does your organization receive support in the area of cybersecurity? If yes, from whom? If not, does your organization need support? Why?

   The majority of our IT is outsourced to external vendors and they support us in this as well.

   Q: Does your organization need the support?

   When IT systems management is done by a third party, it is inevitable that you will also have to discuss with that third party how they have organized things, not just on paper but also in practice. And yes, it can happen that you see vulnerabilities there for example. Together, you must then ensure that you become safer. In our case, I do that for ourselves, but also for other housing associations who are customers there.

9. How does your organization currently stay up to date on current cyber threats? How could your organization stay even better informed about current cyber threats?

   In multiple ways. Firstly, it happens by the information received from external organizations or partners. Secondly, we are affiliated with Digital Trust Center (DTC) and Connect2Trust and from that angle, we also

receive non-public threat information. Thirdly, we also use public sources such as feeds with security vulnerabilities that come in and because I also know which products we use, I can also look at the moment when new threats come in, whether they apply to us.

10. Does your organization work with other organizations in the area of cybersecurity?

    Yes, we work together in Zeeland. We are part of two collaboration agreements. We work closely with Woongoed and Zeeuwland and have a slightly less intense cooperation with the Zuidwest Samen collaboration (ZWS). This includes housing associations such as Oost West Wonen in Middelharnis and Clavis in Terneuzen. Additionally, I am a member of the security special interest group of Corponet and we will be sending out an email to the members of Corponet that we have also started an I-SAC, an Information Sharing Analysis Center, which aims to provide the entire housing association sector with information on information security.

    Q: What does this cooperation look like and how did it start?

    The Zuidwest Samen (ZWS) collaboration has been around for over 10 years, without any formal agreements in place. It started informally and without any legal obligations, but this allows everyone to work together in places where it makes sense. It's really focused on helping each other out and you don't have to participate in everything, but when it's something that affects you, it's a matter of give and take. The hack of eight housing associations in particular has made us more aware of the importance of security and we have worked with VVA and Joanknecht on an incident response plan and we will soon be looking at what other measures we need to implement.

11. Is your organization sufficiently secured against a cyber attack? Why or why not? What still needs to happen?

    I think that you can never be secure enough, you can only do your best to stay one step ahead of criminals. So far we have been successful, but they haven't got us yet. But I don't have the illusion that we can prevent it, partly because you can't do everything, right? And I do see some technical measures that we can still take. But mainly I work on raising awareness among my colleagues by giving them real training, for example, if you receive an email and you have a feeling that something is not quite right, don't click it for safety, but stop and ask for assistance. And the second thing is that I see that the parties we work with don't always have the same drive or focus on information security as I do. I have to be very careful about that, but it does mean that, as you can see from the hack of those 8 co-operatives, even if you have everything in order yourself, an IT service provider can have someone click on the wrong link and everything is exposed, and you can't stop that, except by continuing to talk to those parties and highlighting the risks I see and insisting that they must be resolved.

    Q: So, Commmunicate and collaborate more on that topic, and pay close attention to ensure they have everything in order?

In terms of IT systems management, when it's outsourced to a third party, it's inevitable that you will also have to discuss with them how they have organized things, not just on paper but also in practice. And yes, it can happen that you see vulnerabilities there for example. Together, you must then ensure that you become safer. In terms of communication and collaboration in this area, most housing associations have not only outsourced their IT systems but also their knowledge of it, so they are not empowered to control their vendors. Many housing associations rely on their vendors for IT decisions and might not be able to see what the vendor is not doing or which risks they're taking. This can be a concern because as we have seen from other housing associations, data can be stolen and sometimes even data that should not have been stored in the first place. We need to work together and be aware of these things, to keep ourselves and our data safe.

Q: And you just mentioned that the human aspect is perhaps one of the most important focal points of information security?

Ultimately, that is the most important because the most important firewall is simply between the screen and the chair. The chance that they will exploit a technical vulnerability without the cooperation of a person within is very small, they would really have to break through a firewall or something like that. Most attacks start with a phishing email. Then you have the employee who clicks on it. If you can prevent that, you can simply limit the damage. Two weeks ago, I think, there was an incident at Woongoed in Middelburg due to the alertness of an employee, they were able to limit the damage. It also started with an email. Yes, you really need those employees. Creating that awareness in the organization is extremely important to counter it. As an IT professional, you may assume that everyone will pay attention if they receive a special email, but you should never just assume that. People with different IT skills are working and one person is good at one thing and the other is good at another. You have to help each other to reach a certain level. It is not the intention to do naming and shaming, but to make sure that people will get better from it. That they will think better in the future and it really works. What I see, for example, is that at our organization, even the executive clicked on one of these mails. And that person then screams from the rooftops how important it is for people to realize what they are doing.

12. Is there a formalized (IT) risk management policy in your organization?

    Yes, that is true, we have just redesigned our information security policy. We did this in collaboration with Chapter2 and it has also resulted in a risk management policy and risk classification of business assets. This will be formally established soon and then there will be an annual cycle that will repeatedly review these issues.

    Q: And when does this date back to?

    Just now, december.

13. How are cyber risks identified in your organization

By analyzing the assets of the company, the information being processed and the priority of that information for business operations, in order to establish a risk management policy and classifying those assets according to risk. This will be formally established and reviewed annually to ensure it stays up to date.

14. How is the risk acceptance level (risk appetite) determined in your organization, and by whom?

    The risk management and classification of assets is determined by the management and will ultimately be delegated to the controller.

15. How are risks classified, prioritized, and mitigated (processes to reduce the negative consequences of risks)? What measures have been taken or need to be taken? Are these measures structural? And sufficient?

    That is actually included in the policy that is going to be formalized this month. And when we start using "Fully in Control" next year, we will actually link the measures and risks together, so for each risk you will describe how you are dealing with it. At the moment it is still in Excel Spreadsheets, where the risks are identified and it is indicated what needs to be done and what the current status is. And then you can see if they are still open or not and it will be reviewed periodically.

16. How and with what frequency are risks within your organization evaluated?

    Once every quarter. At the moment, the risk list is updated annually. If actions are identified, they are implemented separately.

    Q: Is this enough at the moment?

    Currently, it is sufficient but that also comes from the fact that the measures that need to be taken in terms of information security are already in place and in some areas, some tightening is needed. Sometimes when you start a new information system, that comes in naturally. In the basics, things are well-organized.

17. Are risks in your organization classified in a standardized way (chance * impact)?

    At this moment, no, because IT risks and other risks are not yet in the same system. But next year everything will be in the same system, so it will be standardized.

    Monitoring and reviewing

18. Is the risk assessment methodology reviewed periodically?

    We need to start implementing it first and then we will evaluate it annually

19. How is the periodic performance of the IT risk analysis ensured?

    Because our control ensures internal audits on the functioning of this system.

    Communication and consultation

20. In what form are the risks reported to management?

    The part of that cycle also includes reporting and that report is discussed within the management team.

21. Is there an action plan / roadmap for mitigating identified risks in your organization?

    That depends, it varies per risk. Depending on what the risk is, it will be assigned to the appropriate person or department to mitigate it.

22. Are IT risks sufficiently covered? Why or why not?

    Basically, it's an ongoing process. You can't say that they are adequately covered. You will always have to keep working on it, because as soon as you think you're done, you have to start all over again. You keep working on it. Last year you could say, "I have implemented MFA. I am done." But now, people are bombarded with authentication pop-ups and you have MFA fatigue. So that's not safe. Now you need to move on to Unfishable MFA, so you always have to take the next step. You will never be done with it. All I can say is that there is enough focus on it. Not that the measures are sufficient, because when something happens, you will say afterwards that it was insufficient. I think that I can say in advance that it is never good enough.

Privacy & information security within your organization

23. How is it ensured within your organization that information is always available (availability)?

    Security measures are taken at different levels and in different ways. People can work from the office and from home. People who work from the office have multiple internet connections available, so if one goes down, the other takes over. We have backup power supplies. We have also installed a fire suppression system in the technical rooms. So if a fire occurs, it doesn't mean the whole building is not available if the connections fail. The next step is to run all our IT systems not in our own building but at external suppliers, in a data center with backup power, cooling, fire protection, access control, redundancy, backups, firewalls, and so on, from redundant facilities.

24. How is the integrity of information ensured within your organization? In other words, how is the information protected against unauthorized or unusual modification or destruction?

    Basically, people are given access to information based on their job function. However, the philosophy of Beveland Wonen is to have a low level of trust within the organization, which means that a lot of information is accessible to everyone. People who enter our organization, both employees and temporary workers, are always asked to provide a VOG (Certificate of Good Conduct). The procedure for creating, modifying, and deleting accounts is handled by HRM, so there is also oversight in that area. People also sign a confidentiality agreement and are trained on how to handle IT equipment. For example, laptops are always encrypted and mobile devices are also secured and the security level of

those devices is monitored to make sure they are always up to date with antivirus. Even with all these measures in place, it's still possible that someone may make an unauthorized change to a document. In that case, we always have backups that can be restored.

25. How is it ensured within your organization that only authorized people have access to information? In other words, how is the information kept confidential?

    When we share information with external parties, on a project basis, through teams or individually, we use Zivver to send that information via encrypted email. We also ask for a second authentication factor from the recipient, and we can also recall a message if it has been sent to the wrong person.

26. How does your organization comply with privacy regulations? For example, by complying with the GDPR?

    The laws and regulations that are specifically anchored in the information security policy and are also named there are applicable to us. In addition, our privacy officer is also our lawyer, so we have also secured the link with laws and regulations.

27. Are all actions in the different information systems controlled (auditability), and how is this done?

    On the main information systems, we have active auditing and logging, which allows us to record changes and also be able to retrieve certain information requests.

    Q: So only on the main systems with privacy-sensitive information?

    That's correct, for example, everything where personal data is stored. For example, on Active Directory, changes to user accounts are also recorded in logs, so they are also retrievable.

    Q: Is there a frequent check on those logs?

    The logs of our internal systems, so where it really concerns audit reports that are periodically reviewed by our control. They have a yearly cycle for that. If we're talking about things like Active Directory and the like, that's only done if there is a need. But that also comes from the fact that it's outsourced to external providers, so we have less control over what they do with it.

28. Are the data and information systems often cleaned?

    We have a DMS, a document management system, and all archive-worthy things are stored in it, on one hand these could be for example rental agreements, and on the other hand it could also be meeting documents where decisions are made or invoices, really all those kinds of things. All those documents are categorized, classified and depending on the document type there is also a retention period and when that retention period has expired, or for example when a tenant's file is closed because the tenant is leaving, that triggers the cleaning process and after that retention period the documents will also be deleted.

29. Are improvements needed in any of the above aspects? If so, which ones? Why?

    When you talk about structured data, like a DMS, it is relatively easy to manage and if you talk about unstructured data, what's in people's mailbox? What do you have on network folders? It's a completely different story. It's much harder to keep it clean, we're also working on that. Only it just takes more time. You really have to develop the methodology to track down information you don't want in there and then to put it in the hands of the responsible department, right? We can clean up our DMS with an GDPR scanner and that can do great things. We're now looking at the front of the process, at the people who put it in and make sure they don't put it in anymore.

    Q: And, how are you tackling the unstructured data?

    We have developed our own scanner to sift through that unstructured data and the next step is to go to the departments and ask them to clean it up, but then we also have to offer them an alternative. We also have to explain. You shouldn't keep this and store it somewhere else. For example, people with documents with passwords. Then you have to say, hey, you can't store that there. Here you have a password manager, but then you have to take that second step. I'm not just about banning things. Let's please look for a solution together, because those people are just doing their work. Not just waving a finger, because in the end you all work for the same organization and try to do it in the way that seems best to you based on the knowledge you have. So if someone else like me says I think it should be done differently, then we should meet each other and look at, how does this come about and how can we help each other improve this?

30. Is the privacy and information security sufficiently safeguarded? Why or why not?

    I think that's the case. Because we have it sufficiently in our sights. The people who work with this information, they know what they're doing, they know what's important to keep information safe, and they're also open to doing things differently. And they realize what they're working on. And also the willingness to adapt and be open to that. Yes, I think that's just a basic requirement to say, it is currently sufficiently secured. But that doesn't mean there's nothing to improve.

Case study interview 4

Your organization in general

1. What is your role in the organization?

   I am the manager of the Corporate Control department at a housing corporation called Alwel. Our department is a staff control that is directly under the management of the housing corporation. I am a corporate controller who is appointed as an independent controller within the organization according to the law. This means that I have a direct line to the Board of Commissioners if necessary. My role is mainly focused on advising the management, both upon request and on an unsolicited basis. Our department is mainly concerned with governance, risk compliance within the organization.

   Q: Can you tell me something more about Alwel?

   We are a foundation that focuses on the social sector, such as education and healthcare. Our task is carried out with the support of the government, but we do have our own resources. We are under the supervision of the government and must account for how we use these resources. We work in three cities: Breda, Etten-Leur, and Roosendaal. We are also a Fusion corporation and since January 2018 we have merged. Approximately 250 to 300 employees work for us, although the number of full-time employees is slightly lower due to part-time jobs. We rent out approximately 25,000 rental units. We ensure that people have a roof over their heads and that the housing is sustainable. This means that we focus on availability, livability, affordability, and sustainability. Our business objectives can be found on our website, where our new business plan can also be found.

2. Is your organization dependent on IT systems? Why?

   Absolutely, I think you know that we were hacked, right? Well, it just goes to show how dependent we are on our information systems. And that doesn't mean that we can't just switch from the knowledge of the process if the systems are not there. We showed that during the data leak by creating more workarounds and making sure to record data in Office packages, of course, and still provide our services. We can somewhat let it continue to run, but yes, we are completely dependent on it. If you see what we already have in terms of digitalization and how we work with it, it is no longer imaginable that we have to go back to another form or whatever. We are, we are very dependent on the information systems.

3. Who is responsible for the following in your organization:
   (a) Cybersecurity (the protection of your digital systems against digital threats),
   Always the board, but in my opinion the responsibility lies mainly with the manager of business operations, who in turn has a team manager of IA to ensure that cybersecurity is in order. This refers to the information security policy that we follow as a corporation. Although responsibility for this has been delegated in the organization, the manager of business operations and the board are ultimately ultimately responsible.

(b) IT risk management (all coordinated activities from the organization to steer and control IT risks),
Within our organization, we follow the so-called '3-line model'. The first line is the operation, the second line is advisory and testing from business control, and the third line is auditing. This team also has a role in setting up security based on risks in the area of risk management.

(c) Privacy & information security (the availability, integrity, confidentiality, privacy and accountability of the information)
The privacy officers are also part of the Business Operations department and are directed by the manager of business operations. They ensure that the privacy of individuals is protected at various levels, such as in processing agreements with suppliers. If a data breach is reported, it also goes through the privacy officers. So they are responsible for managing privacy within our organization.

4. Is this one function or are there multiple roles assigned to a function? Why was this chosen?

   The legislation around compliance, such as the GDPR, has changed over the years and that as an organization we have to respond to this by adapting our internal processes. We have ensured that we comply with current privacy protection legislation.

   Cyber threats and your organization

5. Has your organization been a victim of a cyber attack?

   Yes.

6. If yes, what kind of attack?

   It appears that we were the victim of a cyber attack via a phishing email last year, in which ransomware was installed and extortion took place. This is a form of cyber risk in which the attacker tries to demand money to stop the attack.

7. And what was the damage to your organization in terms of:
   (a) processes?
   (b) systems?
   (c) people?
   (d) finances?

   The damage from the hack was mainly that we had to restart systems, which took time. There was also reputational damage because we were hacked. In addition, there were direct costs, such as the costs for additional communication and privacy advisors.

8. Could you have prevented this attack? If yes, how?

   No. The level of security was in order, but unfortunately you can still be hacked. Everyone can experience it.

9. What are the other lessons learned?

We have recently learned lessons about how we should have a crisis plan and how to shift quickly in any crisis. This was a crisis we had not experienced before, but it is important to act quickly. Therefore, we need a response plan or a business continuity plan that is ready in case another crisis occurs, so that we can shift quickly. At our organization, we shifted quickly and there was a lot of communication with our customers, tenants, and suppliers. All systems have been shut down to prevent further damage. We want to use these lessons learned and share this knowledge with others in the sector, so that they can also shift quickly in similar situations. We will make a separate report for this and other corporations are also interested in how we approached this.

10. Does your organization use cybersecurity frameworks (e.g., NIST, ISO 27001, ISO 27002)? If yes, which ones and why?

    If all goes well, you will also have an interview with Bart next week. He can better provide you with all the information about our current information security policy, which is based on BIC 3.0, a standard for security policy. Bart is also part of the crisis team, so he can tell you everything about how we are currently dealing with the hack and other matters.

11. Does your organization have cybersecurity specialists on staff? Why?

    There will be a new role for a security officer, which did not exist until now, within the organization and also a steering group for information security. Bart can tell you everything about these new roles and how they are introduced in the organization. He has also written a piece about this before I read it to you.

12. Does your organization receive support in the area of cybersecurity? If yes, from whom? If not, does your organization need support? Why?

    We would like to cooperate with the party that helped us with the data hack and also play a role in addressing this issue. We also want to perform and expand this role within our organization and need the support and knowledge to do so. We want to grow with this role within the IA team and also within the organization, because it is clear that it is important to have a security officer when it comes to cybersecurity and cyber risks, especially in a larger organization.

13. How does your organization currently stay up to date on current cyber threats? How could your organization stay even better informed about current cyber threats?

    We have included cyber risks in our fraud risk policy and stay up to date by bringing in knowledge within our team and by emphasizing to our accountant how we have filled this in and how the security is. We are also working on the process of service and training, where there are risks on all kinds of levels. We close accounts based on this.

14. Does your organization work with other organizations in the area of cybersecurity?

We are collaborating with Zayas, another corporation from Den Bosch, because we have a team on two corporations there. The collaboration is mainly to get a broader base and to form a larger, better team. We can also share costs, which is indeed pleasant.

Q: Are there any plans for additional collaborations beyond that? Or, you just mentioned sharing knowledge about the experiences you have had, but are there specific partnerships or more collaborations planned in this area?

For the time being, it is manageable with two co-operatives, but if we get a third organization involved, it will be more difficult to manage on three organizations. We currently have sufficient security against a possible attack. By moving to Office 365 workplaces, we have also raised the security to a higher level, because there are more doors you have to pass through. This does not mean that something can still happen, but it will then be limited to a local area and will not extend to the entire environment or other companies. We will take steps by moving to multiple platforms in the Cloud.

15. Is your organization sufficiently secured against a cyber attack? Why or why not? What still needs to happen?

Yes, we have a risk policy that also includes cyber risks. We have inventoried the risks and this is updated periodically, with the last update in 2021. We are also working on a fraud support program, because as a corporation with a status as an organization of public interest (OB), we have governance obligations including fraud risk management. At the moment, we are focusing on in-depth research into a particular aspect within our operation, which can be in various areas such as cyber risks, but also fraud risks. We do our best to manage these risks as well as possible.

IT risk management and your organisation

16. Is there a formalized (IT) risk management policy in your organization? And when does this date back to?

Yes, we have a risk policy that also includes cyber risks. We have inventoried the risks and this is updated periodically, with the last update in 2021. We are also working on a fraud support program, because as a corporation with a status as an organization of public interest (OB), we have governance obligations including fraud risk management. At the moment, we are focusing on in-depth research into a particular aspect within our operation, which can be in various areas such as cyber risks, but also fraud risks. We do our best to manage these risks as well as possible.

17. Are there subjects that are missing or receive less attention in your current policy? Or are things well organized, with sufficient controls, both hard and soft controls?

That is something we look at during internal controls and audits. Usually these are the areas where we still have to follow up on recommendations or tighten the process. Yes, we also focus on this, but at the moment nothing specific stands out that requires extra attention.

Risk identification, Risk analysis, Risk Evaluation (Risk assessment).

18. How is the risk acceptance level (risk appetite) determined in your organization, and by whom?

    I also deal with determining our risk readiness for various objectives, such as availability, affordability, financial processes, and compliance. We look at where we absolutely do not want to take any risks and where we can take a little more risk. For example, we take a little more risk to achieve our goal of providing housing for our target group. We therefore have a kind of grid with all our objectives, critical success factors, KPI's and critical risk factors. In this way, we look at our risk readiness and determine which measures we can take to mitigate risks. We also look at our gross risks and if these are sufficiently controlled, we do not need to take any additional measures. If that is not the case, we look at which additional control measures we can take to limit the probability or impact of those risks. We look at risks at the strategic, financial, and compliance level, but also at the tactical and operational level. We take into account risks that play a role in the business process and in other areas. Therefore, a lot of attention is paid to risk management.

19. How are do you classify IT risk in your organization? Does it happen in a standardized fashion?

    Yes, we classify risks at the strategic, tactical, and operational level. In addition, we have recorded fraud risks in our business processes and process descriptions, where we have also named the controls. There is also an important aspect of soft controls, such as how we deal with behavior and culture within the organization to manage fraud risks. This means that we also take into account the opportunity and culture within the organization when assessing which risks we run, using the fraud triangle.

20. Are the risks evaluated and reviewed periodically? What is periodic?

    It could be with quarterly reports. Periodically it could also be annual. It could also be per project. It is at different levels.

21. Is the risk assessment methodology reviewed periodically?

    The methodology we use involves assessing probability and impact and taking mitigating measures, as well as determining residual risks and their acceptance. It is a fairly standardized methodology based on a heatmap and focused on paying more attention to the highest risks. We also distinguish between controllable and uncontroll risks and take into account economic parameters and circumstances outside of our control.

22. How is the periodic performance of the IT risk analysis ensured?

    We also monitor risks through audits and frameworks, such as the text control framework and the management control framework, which are focused on fiscal risks and policies. We often create a top 10 or top 5 list of the most significant risks and have risk owners who are responsible for managing the risks. I report periodically on risk management, describing what the risk is, whether the likelihood and impact have changed, and

what additional measures have been taken to manage the risks. This is done in the form of a descriptive report to management and the board.

Communication and consultation

23. Is there an action plan / roadmap for mitigating identified risks in your organization?

    The action plan includes the steps necessary to mitigate risks, such as taking additional control measures, establishing policies and frameworks, or implementing hard controls. We also have various policies within the company, such as procurement policies, to ensure that policy is followed and work is carried out according to certain standards and process descriptions.

24. Are IT risks sufficiently covered? Why or why not?

    Well, the risks mainly involve auditing and business control testing, especially in the field of ICT. This includes checking the presence and status of accounts and reviewing the internal control plan to determine which controls we want to perform each year.

Privacy & information security within your organization

25. Does your organization use a privacy information security standard (ISO 27001, ISO 27002)? If so, which one?

    The General Data Protection Regulation (GDPR) is an important topic that we need to consider. There are different levels that we can aim for in order to comply with the GDPR, the minimum that we have to do is of course mandatory. But we also have the ambition to reach a higher level than what we have achieved so far. For this we will have to do some more work. At the moment we meet the minimum requirements. And when it comes to reporting any data breaches. We have a team that manages these types of issues. We comply with GDPR legislation but we could take it to a higher level.

26. How is it ensured within your organization that information is always available (availability)?

    There are various procedures in place to ensure information security, such as making backups and using a backup service desk. We also work with service providers to ensure that our systems are functioning properly and that we receive a certain level of service.

27. How is the integrity of information ensured within your organization? In other words, how is the information protected against unauthorized or unusual modification or destruction?

    Access control is an important part of our processes. This means that people only have access to the data that they need for their role. We also use role profiles to manage this. In addition, we ensure that current accounts are logged in and out and that everything is well managed. We have a monitoring control measure.

28. How is it ensured within your organization that only authorized people have access to information? In other words, how is the information kept confidential?

    It remains the testing of accounts and that is in relation to the process of joining and leaving the organization. Within our organization, in other words.

29. How does your organization comply with privacy regulations? For example, by complying with the GDPR?

    We just comply with the GDPR.

30. Are the IT systems and all the data that you have in-house occasionally examined and looked at to see what is still needed or can be deleted?

    During the hack, it turned out that we still had a lot of data that was no longer functional and that could be deleted. We now also need to ensure that we clean up the data and remain within the required deadlines, of course we also need to retain data for tax purposes. In addition, sensitive data must be deleted faster. All this must happen in a secure environment. The hack was a wake-up call for us to clean up within the systems.

    Q: And is that being done now?

    That has not yet been addressed. A new structure has been created for capturing and managing data. This is different from before, because we have not transferred everything to the new structure. We now work via MSteams and the file structure is linked to this. The file structure is linked to this. This is a different way of working than before.

31. Are all actions in the different information systems controlled (auditability), and how is this done?

    System logs are important, but it is not necessary to turn on all log files because this can slow down the system. There are specific log files that we turn on for functional purposes.

    Q: Are the logs also regularly checked?

    I know that there are internal control plans to check accounts and that there are specific log files that are checked. However, I cannot say that all log files are checked, but they are used functionally. And checked where necessary.

32. Is the privacy and information security sufficiently safeguarded? Why or why not? Are improvements needed in any of the above aspects? If so, which ones? Why?

    There are always areas for improvement and it is logical to want to achieve the highest level. But sometimes it is also important to consider whether this is still workable. For example, if someone leaves a laptop open and does not shut it down or lock it, someone else can easily access the data. That is why there are also "soft controls" that help employees to adjust their behavior. But the unpredictable aspect is what people do and how they handle data, such as a laptop that remains in a bag or in a car. This is

now being handled better than before. These are all house rules that are enforced within an organization, such as the handling of keys and other items. At the moment I think that the privacy & information and security of this are sufficiently guaranteed. There are authorization, accounts, and password protection present. If this were not the case, we could be called to account for it.

Case study interview 5

Your organization in general

1. What is your role in the organization?

   Yes, I am the manager ICT, and therefore also responsible for security and the resources of the Ciso/Security Officer who is also attached to me.

2. Is your organization dependent on IT systems? Why?

   Yes.

   And why is this the case?

   Well, if I look at what we have digitalized and organized, it is no longer possible to work in any other way to maintain the continuity of your business. If something happens, you would have to do something, but it is no longer possible to return to the situation from years ago.

3. Who is responsible for the following in your organization:
   (a) Cybersecurity (the protection of your digital systems against digital threats),
   The role of our board member is, of course, ultimately responsible, the board member always is. That is actually part of his function. If you go down a step, it is the manager of business services. And then I come as the manager ICT. Actually, cybersecurity is the responsibility of the entire organization. It is also a struggle for us that it is too much tied to a function and not the responsibility of the organization. Yes, I would prefer to see it spread throughout the organization rather than tied to a specific function. Yes, the structure does not serve the interests of cybersecurity.
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks),
   That also comes under me as manager ICT.
   (c) Privacy & information security (the availability, integrity, confidentiality, privacy and accountability of the information)
   Our privacy officer.

4. Is this one function or are there multiple roles assigned to a function? Why was this chosen?

   Yes, I think it has also grown out of the situation. We used to have a legal department. Previously, privacy was logically connected to that department, especially in 2018 with the tightening of the GDPR, the rules and policies that you had to have in place. It was a logical choice to put that under that function, so it is actually not a function. It is a part of a task that they perform. It is a role such as security or finally also a role and not a function within our company. So it has actually grown that way. Filled based on the knowledge we have, yes.

5. If you have not yet been a victim, is there a real threat of a cyber attack? Why?

   Yes, truely, yes.

Q: Why?

I think yes, you can close your eyes and not look at what is happening in the world. You can just follow everything that happens and then you just know. It is not a question of if, but when. And we have continuous discussions about that, also with the DT about how we deal with it and how we are prepared for it? That is why we have a lot of cybersecurity plans to be prepared. We also invested in one and a half years ago because we just see that the threats are real.

6. Does your organization use cybersecurity frameworks (e.g., NIST, ISO 27001, ISO 27002)? If yes, which ones and why?

   We follow an information security policy and plan in accordance with the BIC, which is based on the ISO baseline for information security for housing associations, which is based on the ISO and has been supplemented for housing associations. One and a half years ago, I said, well, this really has to change. We see threats coming towards us. We started with the NIST framework, the Nist cybersecurity framework, because we want to fill it in and take all measures based on that to be ready for a cyber attack.

   Q: Okay, so we started with the BIC and the NIST Framework in the past 1.5 years and they operate alongside each other?

   The BIC is much more focused on organizational policy while we look at the NIST, which is much more focused on cybersecurity and all the measures that go with it.

7. Does your organization have cybersecurity specialists on staff? Why?

   No, not that. I have already followed the necessary training in cybersecurity, but more on the side, not so much to discover it but just to learn what you need to do to implement the cybersecurity framework. The risk matrix, your risk analysis, your BIA Business Impact analysis. Those are parts where I have followed the necessary training to be prepared.

   Q: Do you think something is missing there? Would it be nice to have a cybersecurity specialist on staff or can it be done through training as well?

   Well, yes, it's mainly about, where can you get knowledge when you need it? You don't have to have it all yourself as long as you have a party somewhere where you can get it.

8. Does your organization receive support in the area of cybersecurity? If yes, from whom? If not, does your organization need support? Why?

   Well, we have different parties giving execution to that NIST framework. We are sitting with different parties to gather information, share knowledge, on the one hand with VVA informatisering to come to an incident response plan together. We are sitting with Audittrail to come to a good awareness program. We are now conducting a Business Impact Analysis with Audittrail and we are working with NorthWave on a complete risk assessment to come to a baseline. Where are we now and what are the measures we still need to take to reach a certain level that is

both feasible and user-friendly for us and for the IT user. We are looking for incentives there and we are doing that together with NorthWave and taking all measures against the threats that we see coming our way.

Q: On those different levels, you are looking at whether there are other organizations for support, so you look in the market for a party that can help you where necessary?

Coordination and direction. We do that from our own IT team.

9. How does your organization currently stay up to date on current cyber threats? How could your organization stay even better informed about current cyber threats?

   Yes, that is in various ways. You have the National Cyber Security Center where you get all kinds of updates. We also have a dashboard where all the threads and all the threats come in neatly on our dashboard, so we have a monitor tool where we just, yes, the threads that come our way, they are all there neatly and then you can also plot them on your own vulnerabilities, what does it do in your own environment? So we have a limited dashboard, it's not a SOC. But it is a dashboard where we can discover vulnerabilities and threads. The dashboard is actually the Microsoft dashboard, so the Microsoft Defender dashboard 365 where all that equipment comes together. That's where your applications come together running on your devices, not the applications running in the cloud, because then you really need a completely different solution. It's just your basic device management and everything running on your devices. That is monitored and monitored there. Then we have control, so to speak. And there are also triggers on it. If something happens, signals are given. And that first goes to our outsourcing companies. That is NEH who actively monitors it and yes, we handle other things ourselves.

10. Does your organization currently have a cybersecurity insurance?

    No, we haven't taken one out. The reason for this is that the insurance we had, it stopped and upon investigation of a new insurance, only the policy conditions and the premium were such that we said, that won't benefit us. Uncertainty in the policy and the premium that are just not balanced then we said no, we will invest the money that we now have to pay for an insurance that doesn't pay out. We will use it to optimize our security once everything is in order, yes, then we would like to sit down with a party. Then the development of the insurance may also be a bit further, because so much has happened in the insurance industry in the past year. Now we are only looking at whether the insurers are ready to conclude a good policy and based on the measures we have already taken. It has just been panic football from the insurers in the past two years. But the future insurance will be linked to the risk analysis, where are our risks, where are our threats and which measures can we take to remove them? And if there is still a remainder, should we insure ourselves for that or can we just pay for it? That is the balance that still needs to be made.

11. Is your organization sufficiently secured against a cyber attack? Why or why not? What still needs to happen?

I think we have the security in order on the outside. You always have to be careful with what you say. We have taken a lot of measures in the past 3/4 years to better secure the access to our systems on our network. But, it can always happen, so if you ask what else needs to be set up, we just had a report from NorthWave, so I can answer that very well because it has also been tested. So the security. Well, I think we have it set to green as being in order. Monitoring if it does happen. Well, there's still a big question about how quickly we can notice that a hacker has entered without an employee noticing, right? And saying, I have something weird, but the system automatically detects it and takes measures. Well, we still have to make that step and there is also still one big challenge in terms of privacy. We also see that our systems have too much information that is not cleaned up, that is no longer relevant for our company to do business, but the information is there. That is a challenge and ultimately the access to all this information is too widespread in the organization. That is still a challenge because it would be better organized through classification and other ways, but also by setting up your authorization layer. We are currently working on a business continuity plan and it is currently being gathered in interviews within the organization. In the process, you run the Business Impact Analysis, right? Where do you see the risks and what if, what do you have, what is our plan B? That is our continuity plan and it still needs to be written. An inventory is currently taking place.

IT risk management and your organisation

12. Does your organization use a risk management standard (risk management standards, describe processes and are intended to identify and limit risks)? If yes, which one?

    No, not really on that scale, it's not formalized like that. Of course, we have included in our procedures how we deal with incidents and at what level we eventually go to a crisis team. No, that, that is all described in the procedures. Yes, then you are really talking about your incident response.

Context establishment

13. Is there a formalized (IT) risk management policy in your organization? And when does this date back to?

    I think that's good. We have two things, we have policy and you have a plan. The plan has been updated and approved. The policy has also been re-approved, but not updated. It's strange to say, but we have focused more on updating the plan and the policy has basically continued from the previous year and we now realize from the audit we have done that we need to formulate the roles and responsibilities in the policy more clearly. What is the responsibility of the board member? What is that of the director, what is that of the security or his privacy officer? We now notice that this is insufficiently anchored in the policy document. Yes, well, we will have to do that. That is actually what has come out of the audit that there is actually a lack of clarity in our organization, because the role of the organization and the middle layer is not described in the policy and that is why we now notice that it is not fully alive either. Nobody knows who is responsible for what on this issue, so getting more specific about which

roles or who is responsible for what on this issue and including that in the policy documents.

14. Are there subjects that are missing or receive less attention in your current policy?

    Yes, the responsibility so that a director can say, well, I clearly know where the bar is set for me in this area. But also a middle manager who also knows what is expected of them. That everyone in the organization knows where they stand.

    Risk identification, Risk analysis, Risk Evaluation (Risk assessment).

15. How are cyber risks identified in your organization?

    Yes, we do that based on the fact that we just had a colleague who clicked on an email. Just this morning that is, who categorizes that which is based on our policy is level zero, right? We don't know what's going on. An investigation starts, a critical system is affected, it stays on the device, so ultimately he is. The investigation has remained at level zero in this investigation, because the device has been fully scanned and there is no situation. We have taken all necessary measures. Password reset and everything has been done. It has not gotten bigger than that, but if it were to grow, it would go up to level 3 and from 3 we handle it ourselves with our own security team in our own team. Here the security team is set up and someone starts working on it right away to figure out what's going on. And if it goes from zero to one to two to 3? The other employees come in to assist. From functional administrators to maybe even someone external, who looks at it and from level 4 the crisis team is alerted and then we are here talking about this incident with the entire board.

16. How is the risk acceptance level (risk appetite) determined in your organization, and by whom?

    Yes, that is then, then I think what we are doing now with the Business Impact Analysis, because just to pick up on what is acceptable? What is acceptable? The phone is not working now, but it doesn't work for a day, but it doesn't work for 3 days, what is acceptable?

    Q: Yes, who decides that then?

    The primary processes. We have now brought those into view and based on those processes we are now conducting interviews with managers and employees in the organization, about what it means for their daily work. So if we take the customer contact plan for example, we are really sitting with the employees of our customer contact center at the table and saying, what then? The phone is not working now, what then? Is that a problem for those who are part of those processes? It is measured and looked at in that way to see what is acceptable or not, not the whole thing, but just representatives from the process, key players from the process who are included in the interview.

17. How are risks classified, prioritized, and mitigated (processes to reduce the negative consequences of risks)? What measures have been taken or need to be taken? Are these measures structural? And sufficient?

That is what needs to come out of it.

Which measures to mitigate risks are already being used now?

Yes, there are of course already quite a few agreements made. For example, we already have a social monitoring tool available to see what is happening with the customer, but also with which we communicate with our customers when systems are not working. We have also made agreements with our emergency telephony provider in Hoorn, that is, that is our emergency option for weekends and evenings for emergencies, because there are also agreements there. So we have already done some things. For example, we have at least that system and they have backup plans for other systems. Laptops that are not connected to the network that we can use right away. You name it, so there are some actions, but not yet driven by the results of this plan, but just based on common sense.

Q: Are the measures taken, sufficient?

no, no, no, there is much more to it than that. Look, if the phone doesn't work and that's all nice and well that it doesn't work now. But what if it doesn't work for a week for the customers, they still have problems, they come to the counter or employees go out in the neighborhoods and they are approached. How do you deal with that? Yes, how do you then register it? How do you treat it all? So there needs to be a plan for how you are going to handle things, but if the system doesn't work, you also need a plan for where we write all that down? How are we going to register it? Or are we going to go halfway? Is it with their own device going out into the neighborhoods, are they going to put it on their own private one-drive, so we need to make agreements about that. Do we have a format for that or a separate environment that is made available for employees to be able to continue working in a kind of other teams environment? Depending on the outcome of the BIA, we will look at what management measures we need to take to keep plan B functioning in the plan team without employees looking for their own way out to register or record something or maybe not even record it, causing a whole problem of trying to straighten everything out later.

18. How and with what frequency are risks within your organization evaluated?

    Yes, now we do it periodically. We have a privacy security team that meets every 6 weeks. And we do that mainly focused on the measures we want to implement, but actually we also look back at measures we have taken that have an effect. So periodically we do sit down for this. Every 6 weeks we have a privacy and security meeting, but that does not yet include the whole part of the NIST framework that we are now implementing, so that still needs to be added. Look, the BIC, that's all nicely already arranged, we've been doing it like this for years, so that's all reasonably already regulated with evaluation and periodic meetings, but the NIST framework still needs to be added to that.

19. What topics are missing or less common in your risk assessment and why?

I think that we should focus on how to make a recovery plan once the risk assessment and business impact analysis are complete. We have backups, but how do we restore everything? For example, if our CRM system stops working but our AX system is still functioning, how do we ensure that the information being exchanged between the two systems is synchronized when we restore the CRM system using a backup from a week ago? We have segmented our systems and moved to the cloud, but that has consequences for the recovery plan. It's not just a matter of restoring one system, because the new data in the functioning system needs to be synced with the old data being restored. There are challenges to consider in making this work effectively and I'm still searching for best practices to follow

20. Does your organization use a risk framework (such as ISO 27005, ISO 31000, COSO 2017)? And why or why not?

    No, no, no, we use the ISO from the BIC. Where the BIC is based on but that is the ISO we use, but I think that is a 27001. That is correct.

21. Are risks in your organization classified in a standardized way (chance * impact)?

    Yes, we are working on that. The classification of the risks. We are still looking for the matrix. We have now done the risk inventory in NorthWave and there we get recommendations on how we are going to classify that classification and that has more to do with how much it will cost once a week, you know, the impact and chance. Once we have determined that, it will also be set up in our ISMS system. So that we can apply the matrix to each application and process. Yes, we have a template that we now want to establish and then apply? Yes, to everything that has to do with chance. Yes, exactly. But not only on IT, but also drawing on other risks that you run on your real estate. Just taking you as an example, a wide yes risk is spread, but staying within my field. Then it has to do with IT risks that also affect your real estate. Many of our complexes are secured with a smart access system, right, electronic access. Yes, if it is hacked. It's a serious problem if either all the doors are open or all the doors are closed, then you have a problem, exactly. Yes, it has to do with your image. Yes, I am hacked, but imagine if the access system of your complex is hacked, then as a company your continuity is not at risk, except if you cannot enter your own building. But your impact on your residents who can no longer enter. Or even stronger, that everyone can enter?

    Monitoring and reviewing

22. Are the risks evaluated and reviewed periodically? What is periodic?

    already discussed.

23. Is the risk assessment methodology reviewed periodically?

    Q: You are now still working on a risk assessment methodology and we also plan to take it up again periodically and look at it, is it still correct, do we need to do something else?

Yes, it is also included in the proposal that will come to the management team next week because this session, so to speak, that we have done now to repeat annually to review the threats together again. Are the threats that we see now still the current threats? Or have new threats arisen? It will be evaluated annually. Yes, it has not yet been determined, but that is the proposal.

24. How is the periodic performance of the IT risk analysis ensured?

Yes, that was the problem, that's what I am now, but actually we want this to be much more and that also comes in that piece of policy. How can we make it so that it is not linked to my function or to my person? How can we place this much more organization-wide. That is one of the measures that comes out of the audit, it depends very much on my person, so how are we going to better secure this? So that is a plan, a measure that we want to take up next year and discuss with the Management Team.

Communication and consultation

25. In what form are the risks reported to management?

Look, cybersecurity, I have a meeting with the Management Team every 6 weeks. Then it is about all facets of IT from projects to management and there is security. Is there a particular focus on cybersecurity as a regular part of that.

26. Is there an action plan / roadmap for mitigating identified risks in your organization?

Yes, they are included in that. Yes, so the information security plan, there are all kinds of measures. Those measures are all labeled to people who need to do what and in that periodic Privacy & Security meeting all those measures are discussed with each other. What do you have ready, what do you have and do we do it like this? And all those measures will also be included from the new cybersecurity roadmap. And names are also attached, etc.

27. Are IT risks sufficiently covered? Why or why not?

Not yet. We are still in development. Yes, yes, we are now three-quarters of a year further I think we have made good progress on a number of domains of the NIST framework. Both on identify protect and detect detect we need to take an extra step, but on respond. Now we have made the step, it needs to come into the business continuity plan, but the most important thing for me is detect and recover. Yes, we still need to make progress there.

Privacy & information security within your organization

28. Does your organization use a privacy information security standard (ISO 27001, ISO 27002)? If so, which one?

Only the BIC

29. How is it ensured within your organization that information is always available (availability)?

Yes, that is very difficult, on the one hand, of course, by having systems up, but that doesn't say anything, because the information must be correct and that it is only about availability and not about the integrity of the data. Availability is built into your IT management. The agreements you have with your suppliers, your agenda, your monitoring, availability is actually on the IT side. I think we have that 100% or at least 90% covered in all the requirements we set for suppliers before we do business with them. And the periodic meetings we have with suppliers, the requirements we set. And in addition to your own monitoring and your own service that we have. We have a fully equipped ICT team that can respond to that, yes.

30. How is the integrity of information ensured within your organization? In other words, how is the information protected against unauthorized or unusual modification or destruction?

Externally, I think it is well shielded by what we just discussed. If you look at the integrity of how we handle data internally, there is still work to be done. Yes, because the integrity of our data is on the one hand how we handle it when we talk about customer data at the coffee machine? We have a very nice collaborative environment where people can discuss things with each other in a room. Well, there too. Do you sometimes have the question of, do I want to hear that? So there is something on the side. Exactly the people side and also how colleagues share information with external parties. We have now set up a nice tool from Ziffer, but yes, you have to use it. So on the employer side, knowing what we share and what we are allowed to share. We have not yet set up data classification, right? So there is still something to be gained on that side, but definitely on the awareness side of the employees, but also on the privacy officer role to take ownership of that and do something with it. That role should actually be expanded further and definitely also include this. The privacy role we have now is more focused on signaling. And while you actually expect it to be much more proactive in the organization to do a bit of awareness and be involved in classification or other things where you have authorization, you are much more actively involved and as owner of this, this has to be done by privacy. Instead of signaling and then waiting until one of the managers picks it up, not much happens yet.

31. How is it ensured within your organization that only authorized people have access to information? In other words, how is the information kept confidential?

Yes, we come back to the same thing again, right? You have your authorization matrix and you look at access. That is all arranged from yes, but all the smart things in technology with multifactor authentication and also IP restrictions and I don't know what else, because for conditional access tooling. Right, so you can only get access to our network with a device from stadlander under various conditions you just don't get on that zero trust model, that is very active. And that also applies if devices are not compatible with our security requirements. And then it also doesn't get on the network. That doesn't pick it up either. There is a very real good shell around it, but on the other hand, if an employee has access to the system, they have access to a lot of data that they may not need for their

function. And then I come to the integrity and confidentiality in the end, because you pick up both of those. Do you need that information for your function? Can we not organize it in a different way and there is room for improvement based on the confidentiality of information. So there is still a step to be taken there actually. And we also have no logging on what an employee sees, so how that is controlled is. So you can see that something or someone has mutated it, then you see everything it has done, but if you

32. How does your organization comply with privacy regulations? For example, by complying with the GDPR?

    Yes, I think that is insufficiently safeguarded with us just what I said. It is being signaled from. But not from the GDPR regulations and it also maybe has a piece. We have a new privacy officer and he does not yet have the knowledge at that level. That is where I think it lies. The other privacy officer did have the knowledge, but he signaled based on that knowledge of right, something needs to be done. This is not good, is not compliance, so to speak, but then you just miss the next step. The consequence was not given, so it remains at signaling, so there is still some untapped territory there.

33. Are all actions in the different information systems controlled (auditability), and how is this done?

    We have, well it depends on the systems, we have quite a few different systems. If I really have about our system saved. The most sensitive information customer data is in it right where we are talking about. Well, then you actually have about our Salesforce solution. Every action is logged, right? It is also transparent, clear, so if someone does something, everything is logged. Whatever he does, it is logged. Look at the AX environment, there logging on the crucial financial processes, not on everything. And, that is the controls where the accountant who does our control, periodically checks the logging. Or if it has all been legitimate. He actually does this also on the authorization model. He also still checks if the roles of the authorization match the rules that we have with each other. This is done on a quarterly basis.

34. Are improvements needed in any of the above aspects? If so, which ones? Why?

    Well, in the main improvement that I see, is the better positioning and a solid establishment of the role of the privacy officer overall and that for both your BIA, really on all domains, for confidentiality, integrity, and availability. Because if you have a data leak, yes, the more information that goes out also depends on the access you give to the employee.

35. Is the privacy and information security sufficiently safeguarded? Why or why not?

    I think the organization at the Executive Team level and in our IT team, so to speak. And also in the key players in our organization like HM control legal and privacy officer, yes, then that is sufficiently aligned. If you then go to your middle management layer and to the organization. Then the organization, we do that with awareness programs so that that runs well,

but insufficiently anchored in the middle management layer. They are the employee in the playing field, while they actually have a very different role and responsibility. And there is still room for improvement on that front.

Appendix I - Expert interviews

Expert interview 1

Your organisation in general

1. What is your position?

   My name is Lucas Vousten and I am 51 years old. I studied business economics in Rotterdam from 1988 to 1994 and then studied accounting in Tilburg. After completing my studies in 1997, I immediately started working as an accountant at Joanknecht. In 2009, I went to Amsterdam to study IT at the University of Amsterdam. Since then, I have been focused on IT audit, with a team of about 15 men and women. Our work includes, among other things, annual financial statement audits, ISAE assignments, SOC 2 assignments, DigiD audits, and forensic assignments. We have continuously expanded our work area and IT audit and advisory is now the main focus of our work, with a small portion still focused on IT audits in the context of annual financial statement audits. We have a strong focus on securing digital systems and processes and improving the quality of the information generated by these systems. I am also involved in the collaboration with VVA and I am proud of what we have achieved so far.

2. And what kind of organization is Joanknecht?

   Our company is an accounting and consulting firm with approximately 160 employees in Eindhoven. Our main services are accounting and tax advice, but our fastest growing division is IT audit and advisory. We have experienced significant growth in this sector and cannot do without it. I am responsible for the IT department and we are also active in the housing association sector, along with VVA. Recently, we have contributed to creating awareness, creating incident response plans at a number of housing associations. In the past, we have also been involved with a number of Zeeuwse housing associations due to vulnerabilities in portals that led to data leaks. Recently, we have also worked with a number of other housing associations. Although we are involved with housing associations, this is primarily through the combination with VVA.

3. Are you also active in the housing association sector with your work? If so, do you consider housing associations to be heavily dependent on IT systems?

   Yes, which organization is not?

4. In your opinion, who should be responsible for:
   (a) Cybersecurity (securing your digital systems against digital threats)
   Everyone in an organization, from top to bottom, from left to right, should feel responsible. In a housing association, there are several important parties who are responsible: Ultimately, the CEO is responsible. In addition, the I&A staff member is responsible. Sometimes there is also a separate chief information security officer (CISO) who is responsible for information security. But really, that responsibility should be taken on organization-wide. It is often the

case that the more attention the higher management or the CISO gives to information security, the better it goes. A disaster can help focus attention on the importance of information security.

(b) IT risk management (all coordinated activities from the organization to steer and control IT risks)
That responsibility should also be shared more broadly throughout the organization. The CISO cannot do it alone. It is a business issue to determine what risks come your way and how to deal with them in your business operations. It is not just an IT matter, but something that should be viewed from a business perspective. To get a complete picture of the risks, it is important to have insight into both the internal and external world of the company or organization. It is also important to get feedback from different multidisciplinary teams and from the front line. The risk profile and risk appetite will often be determined by management or the board, but it is also important to listen to what is happening on the front line and how customers are reacting.

(c) Privacy & information security (ensuring the availability, integrity, confidentiality, privacy and auditability of information)
I have difficulty with the GDPR. It's good that there is attention for it, but I don't see the word 'privacy' in the GDPR. But what I really think is important is information security. Privacy-related issues are also included in this. This is not only important to meet the compliance requirements of the government, that's not what it's about, you want your information security to be in good order. You want to protect your crown jewels. For example, I am the CISO at Joanknecht and as such, I would like to know which emails have been sent, whether they contain private data, etc. However, this can be in conflict with the GDPR, as you are then collecting and viewing data that is privacy-sensitive. That is why these roles, of CISO and PO (Privacy Officer) often have to be separated. But on the other hand, I think that if you approach it well as an individual and are well-versed in the rules, the same person can have both roles.
Q: Do you see in organizations that they take the GDPR into account and that it is about 'we are compliant' and that is not much more done with it?
It is approached in a limited way. They need processor agreements and processing registers in order to act within the framework of the legislation on the processing of personal data. They let it lie for 3 years and maybe look at it again then. But there is more to it than just drafting a privacy statement on the website. It is also about taking measures to protect information security.

5. Do you often see this as one function or are there often multiple roles within a function? Why do you think this is chosen? How would you like to see it?

   If we look at it very purely, privacy would come under the privacy officer. The chief information security officer (CISO) is also responsible for

security. I have no objection to these roles being combined, as long as it is approached in a pure way.

Cyber threats and your organisation

6. Is there a real threat of a cyber attack on housing associations?

   Of course, yes. A. We've seen the examples. B. Why wouldn't housing associations be interesting? C. Why wouldn't any organization, large or small, be interesting at all? So I think all organizations are interesting because there is always something to be gained.

7. And what could be the damage to an organization in question in terms of:
   (a) processes?
   (b) systems?
   (c) people?
   (d) finances?

   You have also had business interruption, which has prevented you from invoicing, such as with the housing associations, which were in the news last year. Rent collection may not have been possible or timely, resulting in a missed year and reputational damage. This is not a one-time problem, as once an indexation is missed, it can continue year after year. In addition, there are the internal time and costs involved, and the uncertainty that this may cause among employees. The cost of research and the loss of personal data and its consequences are also important factors to consider. It is clear that the consequences of business interruption are very diverse and can extend in various ways.

Cybersecurity

8. Do the housing associations you have worked with use cybersecurity frameworks (such as NIST, ISO 27001, ISO 27002)? If so, which ones and why? Do you think housing associations should work with these frameworks?

   Many people were already familiar with ISO, but NIST was still unknown to them. We have also made use of the NIST in the ZWS collaboration. To increase the awareness by using the NIST and to think about the current position of the individual organizations and how they relate to others. This has helped them to become aware of the risks that may arise in the long term and to determine which priority they should give to them. So the applicability of it is certainly present.

   Q: You began your answer with 'now it is' to indicate that this is now the case. Why do you think the shift has now been made to a NIST?

   Yes, because organizations have said that we needed to do something in case of a disaster. It might not have happened otherwise, although there are people who look further than their nose is long. The trigger was that something had to be done, because there had been a disaster at a number of other organizations and they had to act. There is a large knowledge gap between different housing associations and businesses. Some have pioneers who are more than averagely concerned with these kinds of things or who are interested in this matter and seek out information and

knowledge, while others have less affinity and do not seek out new knowledge and information as much. That also plays an important role in how organizations ensure that they receive sufficient input to be able to take all risks and possible measures.

9. Do housing associations often receive support in the area of cybersecurity? If so, from whom? If not, do housing associations need support? Why?

   They need the support because the knowledge is often not present. This applies not only to the story landing, but also to different target groups landing. We are talking about the strategic, tactical and operational level and all these levels must be fed with the right information, so that, for example, the board of directors can also fulfill its role. At the tactical and operational level, people must know how the measures can be taken and how it works. The management must also be fed with this information to function properly.

10. Are housing associations more frequently cooperation on the area of cybersecurity?

    I know from the past that the Lente initiative once originated in Brabant. In Zeeland/Brabant there is a cooperation agreement ZuidWestSamen, in which cooperation in this area has been entered into. I am not familiar with other collaborations in the Netherlands.

    Q: As organizations increasingly collaborate to solve problems, do you think this is a positive development?

    In general, it is a positive development when collaborations are entered into, especially on a subject that is not 'core' to the business. Within housing associations, this is also of added value because business processes and systems used are often also very similar to each other.

11. How does your organization currently stay informed about current cyber threats? How could your organization stay even better informed about current cyber threats?

    Good question. Joanknecht has a number of pioneers who collect interesting information through various sources, such as the Digital Trust Center and NCSC, Security.nl. We also stay up to date on acute current threats but also provide depth through training and courses. In addition, we actively take knowledge of digital attack techniques by participating in challenges, which have a fun component, trying to get as high as possible in the ranking. But of course there is also a serious component to it, because you get very concrete indications that allow you to see what is possible.

12. Does your organization work with external partners on cybersecurity?

    Yes, you can't have all the knowledge in house. Sometimes we also involve lawyers in forensic investigations if there are problems with subjects such as the GDPR. We seek cooperation with organizations that have the necessary knowledge in house to tackle specific subjects and work together. And that is done reciprocally on the market.

13. Are the housing associations you have been at sufficiently secure against a cyber attack? Why or why not? What still needs to happen?

    Yes, it is a difficult question to answer because I don't have enough information to make a statement. In general, I think that there is still a lot to be gained in the Netherlands in terms of cyber security. Some organizations are better prepared than others. In our audits, we see that good password policy is not always properly implemented and the use of MFA (Multi-Factor Authentication) is not always used. Traffic from outside to inside is also not always monitored with IPS systems, SOC systems. It is also important to distinguish between the threat from outside and from within. There are also small criminals within an organization who empty the hard drive just before the end of their employment and take it to a competitor. Misuse of rights within an environment to transfer money is also often made. So it is variable whether companies and organizations are well prepared for cyber attacks. One aspect that receives little attention is being prepared for an attack. It is also important to consider what to do if personal data has been stolen. It is also important to consider the consequences for the reputation of an organization if an attack takes place. It is therefore important to be prepared and to know how to respond if it happens. What we have said in the ZWS cooperation agreement for housing associations is: it is important to think about what to do if it happens. It is also important to have a good crisis structure so that you can respond efficiently. It is also important to have clear who can do what in a crisis situation. What we have advocated in our incident response plans, as they also exist at the different housing associations, is to use a BOB (IJD in English) structure, Image formation, Judgment formation and Decision making. First, take a good look at what you know for sure, what you don't know and what you doubt (image formation). You then look at

IT risk management and your organization

14. Do the housing associations you have been at use a risk management standard (risk management norms, describe processes and are intended to identify and limit risks)? If so, which ones?

Context establishment

15. Is there a formalized (IT) risk management policy at the housing associations you have been at? And when does this date from?

    If it is already there, it is often the last thing. It is important to regularly review how you divide your tasks and whether you are doing enough to keep your household running smoothly. It is recommended to do this at least once a year, and perhaps more thoroughly every two years. But it is also important to be continuously alert for potential threats or problems. When you look out your window, what do you see? What threats are there in the outside world that may affect your assets, such as the applications, applications and hardware you use? Keep an eye on these threats to make sure you don't unnecessarily risk danger. So you will have to look at it continuously and therefore look outward to gather information. Your risk profile can also change over the course of the year.

Risk identification, Risk analysis, Risk Evaluation (Risk assessment)

16. How is the risk acceptance level (risk appetite) determined in housing associations, and by whom?

    Senior management should look into this.

    Q: Is this already often done in this way in organizations?

    It is good to have a discussion about this. For example, to discuss what is done in the case of an attack such as Ransomware. Some say never to pay, while others suggest paying for the key to solve it. However, it is not so simple because there are multiple parties involved and there are different interests at stake. There must be consultation between the experts, such as the CISO, risk manager and FG (privacy officer) and the business. Ultimately, senior management will have to make a decision on what to accept and what to insure, and where we want to take which measures against.

17. How and with what frequency should the risks be evaluated?

    We were just talking about reviewing at least annually and in between based on current events.

18. What topics are missing or less common in risk assessments and why?

    Information security is like a tripod. People, processes, and technology. If one of the legs is not well fed or highlighted, the tripod can wobble and fall, just like a person can fall off a tripod if they are not sitting properly. It is important to hold all three legs of information security firmly to prevent falling.

19. Are risks in housing associations classified in a standardized way (chance * impact)? If not, should this be done?

    I don't think there is a clear-cut answer to that. I think the one who is more mindful and deliberate about it will probably handle it better than the other. So there is no clear-cut answer to that.

    Monitoring and reviewing

    Communication and consultation

20. In what form should the risks be best reported to management?

    There are risks that we need to consider. It depends on the audience we are dealing with how we can best convey our message. This also depends on the form of the message. We have recently spoken with a number of IT parties about the archetypes of people and how they have different drives as humans and how they deal with a message that is brought to them. For example, a stereotypical accountant who is focused on covering risks and wants clear information, while someone who is commercially driven wants to know how to persuade their customers of the measures they have taken. It is important to take into account the recipient of the message and make sure the message actually comes across. However, it is not always obvious to stand still and it is also important to take into account the relationship between the sender and the recipient of the message. It is

advisable to ensure that the message fits the personality of the recipient, so that the message comes across better and no conflicts arise."

21. In your opinion, are the IT risks within housing associations sufficiently covered? Why or why not? What still needs to happen?

    Inconsistent. Some organizations are working on this. We conducted an assessment for a housing association in the area a year ago and it was meant to be revisited annually. However, some people who were involved in this have left, causing it to slip. It is a shame that people are dependent on this and more needs to be done to fully take it up and keep working on it annually. It is important for organizations to regularly hold up a mirror to themselves.

Privacy & information security within your organization

22. Are privacy & information security standards (ISO 27001, ISO 27002) currently being used in housing associations? If so, which ones? If not, would you recommend this?

    The BIC has been brought forward by Aedes and I think that is a good development. But the GBV (Gezond Boeren Verstand in Dutch)(common sense) method is important because it is about thinking in scenarios and considering measures based on what can happen rather than just complying with standards and having a risk analysis. Sometimes too much emphasis is placed on complying with standards instead of the substance of the risk analysis. It is about substance, not form.

23. How can housing associations ensure that information is always available (availability)? Is this already being done well?

    Information security encompasses the availability, integrity, and confidentiality of information, also known as the CIA triad (Confidentiality, Integrity, Availability). There are various measures in place to ensure that this information remains available at all times.

24. How can the integrity of information within housing associations be properly ensured? In other words, how is the information protected against unauthorized or unusual modification or destruction? Is this already being done well

    It is completely dependent on the risk analysis and the measures that are taken. There is no one-size-fits-all answer to this question.

25. How do housing associations comply with laws and regulations regarding privacy? For example, through compliance with the GDPR? Is this already being done well

    No answer.

26. Are all actions within housing associations checked in the various information systems? (Auditability) and how is this done? Or how could this be done?

    There are several ways to check to see if everything is going well. For example, an internal audit tool can be used, or external help can be

enlisted, such as a BIC or ISO. An accountant during the annual financial statement audit can also check certain aspects related to the numbers. And not just limited to the numbers, but also the information security aspects.

27. Are the information systems at housing associations regularly cleaned up? Irrelevant information removed?

    It varies from organization to organization. However, it is important to keep in mind that some information may need to be retained, for example, because it is necessary for future checks. So it depends on the organization what needs to be done with the data or information that is collected. But you can't lose what you don't have.

28. Is privacy and information security adequately safeguarded within the housing association sector? Why or why not?

    It is important to thoroughly and in-depth review the risk analysis. It is also advisable to review agreements with suppliers to determine where the responsibility lies when outsourcing a lot. We have noticed that there is often overlap in expectations of responsibilities, which leads to gaps where no one does anything. That's why it is also important to think about disaster scenarios and to practice them, so that we are prepared if they occur.

Expert interview 2

Your organisation in general

1. What is your position?

   I am a business consultant. Specifically at VVA, where I am currently working on the topic of security and privacy. As an advisor, because my project is mostly advisory projects. Well, a large part of my time is spent on this topic, advising clients on how to deal with information security risks and providing products and services around it, as well as on the subject of privacy. It's about the GDPR. So we work for housing associations, but also some other organizations. I am also currently working with educational organizations. And for example, municipalities.

2. Do you consider housing associations to be heavily dependent on IT systems?

   Yes, definitely. Well, not 100% dependent, but they are certainly dependent for a significant portion, actually for the majority. In fact, almost every housing association outsources a large part of it. When it comes to office automation and really the entire network, it is often managed by a service provider, an IT service provider/hosting party/service provider, whatever you want to call it. And in addition, well, they make use of various systems for the execution of processes, ERP's, DMS's, and other applications. So no, strongly dependent on IT, absolutely yes.

3. In your opinion, who should be responsible for:
   (a) Cybersecurity (securing your digital systems against digital threats)
   Ultimately, the CEO is responsible and they will formally be that as well. But I think it's much more important that responsibility is also taken. And actually, it starts at that level. And of course, some responsibilities must then be delegated to other members of the management team. So it must be strongly anchored on the business side and that you also have a functionary who facilitates a number of things and, of course, can advise from expertise and implement things. Do you need a role for that, the security officer or whatever you want to call him, the CISO or ISO? But that person should not be the one responsible for it.
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks)
   And I really think that is something that fits perfectly with what I just said about the management team. In a joint responsibility, because making one person responsible for security or risk management in the field of security is really something that concerns the entire organization and must be addressed from the top. Yes, responsibility really lies at the management team level with the board also closely involved.
   (c) Privacy & information security (ensuring the availability, integrity, confidentiality, privacy and auditability of information)
   Well, for the implementation of privacy and information security, you have your functionaries for that. So, giving implementation, but also jointly developing policy and implementing policy. Do you

need a role for that, the privacy officer, for GDPR, privacy-related matters and the security officer for information security matters? That role could also be combined into one function. But they are really two different roles. So that person should be responsible for implementation, but for setting up the information security and privacy organization, determining policy objectives, determining the risk appetite, and ultimately, assessing certain risks, which will ultimately lead to policy and a plan being developed and implemented by the privacy and security officer. Yes, the first part, setting those frameworks and establishing that organization, will have to be at the level of the CEO and the management team.

4. Do you often see this as one function or are there often multiple roles within a function? Why do you think this is chosen? How would you like to see it?

Yes, it depends a lot on the size of the organization, right? So you have cooperatives with only 10 employees. So small organizations, up to larger organizations with 300 to 500 or more employees. Most are somewhere in between, I think, medium-sized housing associations with around 50 to 200 employees. Yes, the smaller it is, the more likely those roles are carried out by the same person. And the bigger it is, the more you can divide and assign those roles to different functions, and it is also necessary because it becomes more complex as the organization grows. Because they also have more to manage in terms of risks and measures. And there is a higher level of maturity, so they also realize that they need to do more. And then you often see that multiple functions are created to take on such a role instead of it being carried out by the same person. And you see that in smaller organizations, where you are responsible for privacy or security or something. And I am also actually responsible for the entire business operations and sometimes I also do control. Or someone determines the policy, implements the policy for a part and also checks the policy. Yes, and sometimes it is almost impossible in a small organization, so it is also understandable. But at the same time, it is also a risk.

Q:And how would you suggest that the division in roles and functions is made?

Yes, to some extent, yes. You have to try to separate the development of policy, the implementation of policy, and the control of compliance with the policy as much as possible. And that actually also happens in general, so then you see that the colleague who is responsible for implementation is not responsible for control, and a controller is dealing with it, but at the same time, such a controller often has very little knowledge of information security and is actually not able to perform an audit, an internal audit, on what has been done and therefore there may be separation, but there is ultimately not the quality needed to do what is necessary in your plan-do-check-act. So, but that separation should at least be there. So what do we think we need to do? How are we going to do it? Who does it then? And who checks it in the end? It should be separated in both information security and privacy, and then, in my opinion, you can both have information policy and privacy in your portfolio, because they really have

a lot to do with each other. If someone has sufficient knowledge of both, then I generally see no problem in taking on both roles.

Cyber threats and your organisation

5. Have you ever worked with a housing association that has been a victim of a cyber attack?

   Yes.

6. If so, what kind of attack?

   Well, it recently happened, so it was one after another a business email compromise. That means that there has been unauthorized access to a mail account. That was an attack that was successful, so it was determined that access was gained. Of course, housing associations face numerous attacks every day, from phishing to attempts at hacking, exploiting vulnerabilities, etc., so that is always happening. And of course, earlier this year, eight housing associations were affected by a ransomware attack on their IT service provider. Yes, for that we were also involved from VVA in the recovery process and in particular in setting up the response in the right way. So we were involved in crisis management

7. And what has been the damage to the organization in question in terms of:
   (a) processes?
   Well, the damage on the IT processes has been such that they were interrupted for a long period of time. So the business continuity and ultimately the IT continuity were disrupted. In fact, it was simply not available for a longer time, I'm talking about weeks or almost months. So there was either no availability or very limited availability. In which the housing associations had to be able to carry out a business process without the support of, well, the IT, which had an impact on the IT environment and ultimately on the processes and continuity of the business.
   (b) systems?
   (c) people?
   (d) finances?
   There are various types of impact that such an attack brings, of course. So you have impact when it comes to the business operations, but also impact on other types of damage. That naturally occurs and then we quickly talk about financial damage, of course. That occurred. That had an impact, because there was also a ransom demand at that moment and a business decision had to be made whether or not to pay and the costs had to be made, etc. So that had an impact on it. Well, an impact on the organization and on the people in the organization who work. So a stressful time, a time of uncertainty, and also for those who were closely involved in the handling of the incident and a hectic period that they had not experienced before. So you can also imagine that there was also a large mental impact. Not only among the employees, but also among those involved in the data leak. From who was the data that is now on the street? Yes, that made them worried too, are my data now on the street? And what does that mean, do I have to

worry because it will be misused? So yes, the impact was on various levels.

8. Could this attack have been prevented? If so, how?

I think every attack can ultimately be prevented. But then you have to be aware on the other side that no attack can be prevented. If you look at a... we might have to be somewhat careful with what we release about this specific attack, because the evaluation and ultimately the publication about the circumstances and also the causes etc. is not yet public, but yes, I can already indicate that there are sufficient signals that are not just signals, but are factual observations. Yes, that there were a number of things that were not properly arranged. And so on the side of the provider who had to take a number of measures to prevent access. So yes, we already know that there were also shortcomings. At the same time, yes, did you have that? That is now what is most likely and I have to continue to express this cautiously. Of course, you always have to be aware of the hacker's entry point. Yes, that no security guarantees 100% safety and security, so yes, it could have been prevented. I think in this specific situation, yes, it could have been prevented based on the specific attack that was committed here and the way in which access was gained to the network.

9. What are the other lessons learned?

Yes, they really go a long way, especially in terms of everything that is affected. So the lessons learned in prevention, of course, there are a number of lessons learned that can prevent these kinds of things from happening. You just have to take a number of basic measures that make it much more difficult to get access. You have to make sure that you have the right monitoring in place to detect suspicious activity in time. Looking at the inventory, it's probably step one that follows prevention and detection, you also need to know what processes and business assets we have out of sight and especially in a situation. And you need to know what we have now. Because if you don't know what you have, you can't secure it and especially in a situation where you don't exactly know where they have all been and you are doing an analysis, it is very useful to know what we have in terms of IT systems, hardware, other IT components, applications, data, of course, where is it all exactly? You can only do that analysis well if you have a complete overview and if you also decide later on, a week later, how we are going to bring everything back online if you are lucky to get to that point. You can also make a decision about which systems are most important for you to work on. So that's the inventory side, I'm actually going through the NIST framework, along the inventory to identification, but you eventually get to prevention and detection and respond. Yes, there are a lot of lessons learned there. You can prepare for such a situation, that is actually the most important lesson we have learned, that you can practice such a situation and it is extremely helpful if you know what is coming you in the hectic period shortly after such an incident, you're in a crisis phase and then knowing who does what when and with what is actually the basis for knowing that and who is also allowed to make decisions, because you will have to make a number of key decisions. If you've already documented that, then it's actually known to everyone.

Then, then you have a huge head start on organizations that haven't yet done that. They also have to do that, on top of all the hecticness that is already there, all the tension, but also all the question marks and all the work that has to be done to deal with such an incident and to try to mitigate the consequences as much as possible.

Finally, well, come on recovery. Well, we're coming to the same point as we just did with the inventory that you also know. Well, how are we going to restore things? Do we have plans for that lying around? Can we even restore things, do we have backups, do we also have a fallback environment if it is necessary to continue running shadow processes, for example, to allow the processes that we just mentioned that have been interrupted to continue, etc. Yes, the number of lessons learned that we have also recorded. I'm missing a lot of them, I think now in the story, but I think that's the most important and that ultimately a large part of it in a crisis situation revolves around communication both internally and externaly. That is about 80%, I think, the entire crisis phase and, um, those first week or two weeks after you've been hacked, right? It's the communication in the structure and the collaboration between the team that is dealing with it. Having good short lines, having a good consultation structure, having good documentation of what you discuss with each other, keeping logbooks. Yes, that is really key at that moment, because so much information comes by that you have to know yourself well. Who needs what information at what moment to be able to take the right actions and decisions and putting structure in place when to set it up. Yes, that's really what the crisis manager takes on, so that's also very, very important to set up well.

10. Is there a real threat of a cyber attack in the housing association sector in your opinion? Why?

Absolutely, it has been long thought that housing associations certainly cannot remain unscathed, right? So they are definitely a target and an interesting target, and certainly. So that fits in with the question that was asked earlier about how dependent housing associations are on IT and therefore also on IT suppliers and service providers. Yes, there is a big risk there, so outsourcing IT became the norm in the housing association world last year? Well, not nearly, but that also means that it comes with a responsibility to know with whom I am working here and how can we ensure that it is going well? Because outsourcing your IT does not mean outsourcing your responsibilities, that the IT and therefore your data, etc. that are processed by IT parties are well regulated, then you remain responsible for it. Then you have to stay in control and that is precisely where the risk lies. We have also seen this with the hack that was described, that the housing associations themselves may not be the directly interesting target, but rather the suppliers with which the housing associations cooperate. And so these suppliers then work with numerous housing associations or maybe even all kinds of other customers that they also serve with their IT services. Yes, that is an interesting target for a hacker, because then you have a number of customers who are affected by it, with which you can even extort not only the IT service provider that

would have been hacked at that moment, but also all those other customers, so it really creates a supply chain effect in your hack. Yes, that is an extremely interesting target for a cyber criminal. And yes, we have actually just established that housing associations are very dependent on this, so it is just a risk. Yes, and it will not just go away. Let's move on to the part about cybersecurity. That is on the side of the housing associations.

Cybersecurity

11. Do the housing associations you have worked with use cybersecurity frameworks (such as NIST, ISO 27001, ISO 27002)? If so, which ones and why? Do you think housing associations should work with these frameworks?

I think the most common one is ISO 27000. Two, specifically, one but two when it comes to risk analysis and taking measures, because the baseline information security for housing associations, the BIC, is based on it, so that is actually an ISO 27000 translated into the housing association sector. The translation is not very big at all, so it is actually almost one to one with ISO 27000 One and Two, so we also ask for that. We actually see it especially when we look at housing associations. We also increasingly see the NIST coming up. That is also what is mostly used or in combination with the ISO 27000 series, so that in the field of information security. Yes, and when we look at the privacy side, then it is the Aedes route planner that has been developed for this. The GDPR Route planner, the GDPR itself is of course, in a sense, other frameworks that we also work with as housing associations, right? A data protection officer who is not mandatory for housing associations, but some housing associations do have one. We often see Norea coming up there as well, the Norea privacy framework. That is actually an audit framework with which you can test to what extent you comply with the GDPR. So these frameworks are the most common in the housing association world.

Q: Why do they work with these frameworks?

Well, I think the ISO is of course just the European standard in the field of information security, so you see that in every sector. The healthcare sector uses the NEN 75010. That's of course just derived from the ISO 27000. The BIO is also based on the ISO 27000 and the BIC too, so I think it's mostly that it's the most well-known and also a very good, comprehensive standard. Framework, so yes, that's the main reason it's used. You now see the increasing use of the NIST, and I don't really know why that's happening, but I have a suspicion, which is that it's perhaps a little more compact and clear. It shows a number of things that are important for preventing cyber attacks and what you should do if you are affected. I just mentioned those 5 pillars that are in the NIST cybersecurity framework, and I think that appeals to smaller organizations. I think the ISO is quite extensive, so going through all of it can be quite a lot of work. The NIST helps by allowing you to pinpoint and highlight the things you need to work on, and it helps create a common language. It's often used that way and then maybe later on they'll take a step towards the ISO. But the NIST is becoming more well-known and also more accessible. It's American, so

they know how to make it more commercially appealing and also visually appealing by bringing it down to basic things, including those 5 pillars of the NIST. It really covers a lot of things, so ultimately it's not necessarily smaller or more compact than the ISO, but they've managed to bring it to a level that's understandable.

12. Do the housing associations you have worked with often have a cybersecurity specialist on staff? Why? If not, should they have a cybersecurity specialist on staff?

    No, not often in cybersecurity specialist, because the question is, what falls under cybersecurity specialist? Yes, ultimately cybersecurity is maybe nowadays a bit of a popular name for information security. So basically everything that cybersecurity deals with should also be dealt with by an information security specialist. So it ties in with the question you asked earlier about what such an organization looks like and what role you have. Within such housing associations, you often see that responsibilities for information security and privacy are assigned and they are also concerned with cyber threats and cybersecurity. So yes, we see that responsibilities are assigned and carried out properly. That's not always the case, so there is a difference between assigning those roles and carrying them out properly. So that's what I observe.

13. Do housing associations often receive support in the area of cybersecurity? If so, from whom? If not, do housing associations need support? Why?

    Yes, definitely good, because it brings up the point of the larger and smaller housing associations, right? So the larger ones are more capable of having that knowledge in-house, while the smaller ones are less so and it would be good for them to get advice because they are certainly not, well, not interesting enough for, well, because you can also just be connected to an IT service provider that could be a target and you yourself could be. So it's good to get advice on that. So yes, then to bring the knowledge in-house by hiring someone. That would be worth recommending in quite a few cases, yes.

14. How does your organization currently stay informed about current cyber threats? How could your organization stay even better informed about current cyber threats? How could housing associations stay informed about current cyber threats?

    There are various ways you can go about it, aside from lucking out and having a colleague who has an affinity for it and enjoys educating other colleagues. At the sector level, there are also some initiatives. Aedes also has a collaboration with Corponet. In the past, we at the VVA were also involved in that, which is the cyber security or information security Special Interest Group where housing associations can be members to exchange knowledge and work on practices that can be applied in their own organizations. So it's a platform where you can join to bring knowledge in-house, and in addition, you can also join various national initiatives that are available. I don't see housing associations being very active on platforms like Digital Trust Center, for example, or through social media, but I do see some movement at the sector level and I also see housing

associations seeking each other out. At the VVA, we facilitate that, so housing associations collaborating in certain regions, for example, Zeeland is a region where there is a lot of collaboration on this theme in order to move forward together and also bring knowledge in-house together, because if you have to pay the costs together for an interesting speaker or an expert in a certain field, it's more attractive than having to do it alone. So you often see regional initiatives focused on trying to keep specialists within housing associations who are working on the subject up to date.

15. Does your organization work with housing associations on cybersecurity? Do you see many housing associations working together or seeking partnerships in the area of cybersecurity?

    So perhaps I've emphasized enough that I do see good initiatives that we at the VVA also try to encourage. At the sector level, there are indeed initiatives in various places. I mentioned the SIG with Corponet and Aedes, but if you look at other sectors that may also be at greater risk and are more mature in terms of security, we have to be honest and say that housing associations are generally less so, but they can certainly take examples from them. For example, I'm talking about the information security department of the Association of Dutch Municipalities, where you see how they set up collaborations and really work on things together for the sector, where all municipalities can join in and benefit. In healthcare, there is the Z-Cert, which was established so that all healthcare organizations and central points can contact them if they are hacked. So these are also initiatives, and apparently in non-profit sectors where you don't have competition and can therefore learn from each other for free and join forces, this definitely applies to housing associations as well. It's an opportunity that has been around for a while but hasn't been taken up and not at the sector level either. For example, it would be valuable for a housing association association like Aedes to collaborate with the Association of Dutch Municipalities because they are organizations that are similar in terms of information security departments. y collaborating and looking at what they already have, we can learn from them and implement more practices in the housing association sector. We can be more proactive in identifying risks and setting up a platform together. This is something that is particularly suitable for a sector organization like Aedes. Unfortunately, it does not yet exist and it is not in my knowledge if they are working on it. However, I hope they are and I would like to contribute to it. This would be a step forward.

16. Are the housing associations you have been at sufficiently secure against a cyber attack? Why or why not? What still needs to happen?

    In general, I don't think so. Uh, so I think that we. I just called it like housing associations still have some catching up to do. There are also exceptions in adulthood on this topic, so some have really got it together. I also think that many housing associations struggle with this topic and that is very understandable. It is also not something that is easy to understand for everyone and it has also gone fairly quickly in recent years. As more and more threats come our way. And yes, the capacity is often not there within the housing associations to deal with it, so. Yes, it is challenging

and at the same time it is a risk if you don't tackle it. So I definitely see that housing associations still have some steps to take in adulthood. That is actually the situation at the moment.

IT risk management and your organization

17. Do the housing associations you have been at use a risk management standard (risk management norms, describe processes and are intended to identify and limit risks)? If so, which ones?

    I can't judge all the risks, right? Because, I think we just talked about security and privacy risks and I think that is limited. I think it may be used in certain housing associations where information security is often a part of it, but I think that will be the minority, right, that it is generally limited. I think it is mainly IT risk. And especially if we then go to a, well, a detail level, so to speak, deeper on the security level, there is little use of frameworks and. Yes. Apart from the frameworks, I think that risk management in the area of security and privacy is often not given enough attention.

Context establishment

18. Is there a formalized (IT) risk management policy at the housing associations you have been at? And when does this date from?

    No, I don't think so, no, so I think there is information security policy. Often in the information security policy there are a few things that we do. And risk-driven, that we look at risks, that we continue to analyze them, etc., so there are some things written down, but I don't think there is then also a structure or approach that describes how we deal with those risks. How do we manage them now and how do we continuously weigh them properly? So that in general, I don't think it is or not enough.

19. Are there topics that are missing or less common in the policy and why?

    It is often information security policy, we have, yes, we have okay, what measures are we going to take, then it is, then often thought is given to what are we going to do? Do we often use a framework like ISO 27000, the BIC, then we will run through it, because it actually prescribes all kinds of measures that should be taken, or perhaps should be taken if there is a standard present in order to meet the standard. And then we inventory and then we do, this we don't do, this we do, we don't do. Yes, we haven't been asked. Yes, why do we do it or not? And maybe it's fine Why we don't do it, but maybe it's the other way around, yes, why don't we mention certain things that we should do and to what extent then? In what situation then not? And then you are actually talking about. Yes, which risk assessments do you make to take or not take certain measures and that step is often skipped, yes, can you make that assessment, it is often not made, not all of them, not from a risk approach at least, and that assessment or maybe made based on the finances of, well. Or maybe other arguments are used to explain why you do or do not do something. But yes, is it enough to look at it from a real risk perspective? I don't think so.

    Risk identification, Risk analysis, Risk Evaluation (Risk assessment)

20. How are IT risks identified in the housing associations you have been at?

    In any case, not enough, then I think if it happens, yes, then it is often done using such a framework, right, so then what is often done. What I see is that the ISO is used, the BIC, and there are all kinds of things in it that you should do. And then often a risk is mentioned for why you take certain measures, what the risk is if you don't take a certain measure, right? Of course, that is a risk in itself if you don't take certain measures, but maybe it is no risk at all to take certain measures, because you have to do it the other way around. You have to first think about what risks. What threats, what events in the area of cyber risks could happen and how are we going to arm ourselves against them and what measures are needed for that? So often risk is said, for example, we don't have MFA. Oh risk. Because we don't have MFA, right? That is indeed a risk in some cases, because you have certain applications that you really need to secure with MFA, because that is where your crown jewels are. But they give the same answer for a small web application that we use or a shared account of a website that we use where there is really nothing relevant. Are we going to set up MFA there too? No, no, not okay, but why not? Yes, there is also nothing exciting on it. Okay, so now we are making a risk assessment of why you do or do not do certain things, but then you first have to go about an event that could occur, namely okay, that account could be hacked, but what does it matter to us? Every time we run risks on what sensitivity of data and processes we have, is then interrupted and that conversation. That often takes place by running through measures and that is then called a risk analysis. But well, that is actually the way in which cyber risks should be identified and much less from okay, what could happen now, can we reason from events from threats, what are those threats at the organizational level, process level, IT level, and then we also think about measures, but that is what I see a lot.

21. How is the risk acceptance level (risk appetite) determined in housing associations, and by whom?

    Yes, I think it is not determined too often. I think it is also often based on a standard, right? So the BIC, for example, also writes a number of things, so that is also a standard and that is really just a baseline and it is often used to base their own risk appetite on, for example, it says here. We should comply with this and yes, that is then risk appetite complying with the standard and then well, that's good and everything that is extra needed is not done, because we accept the other. That does not mean that it should be enormous, while the standard is only a baseline and in certain situations it really makes sense to take extra measures to protect yourself, that is not seen in policy documents that circulate in the housing association world, which is actually the core of your information security, so I think it happens too often not enough or not at all and it is more the exception that it is done well, then yes, then it did not happen.

22. How are IT risks classified, prioritized, and mitigated (processes to reduce the negative consequences of risks)? What measures can be taken or need to be taken for this? And is enough being done within housing associations to properly regulate this?

Yes, ultimately, if you are dealing with risks, you actually have it. Those frameworks that can ultimately help you to estimate it, right? So the probability * impact method is often used. According to me, they are also standard in the BIC analyses that you have and the scores that come out of them, which give an idea here at least. Where are our highest priorities now and what should we work on to mitigate the risk or to implement this measure? It often comes down to a risk being directly linked to a measure when you take it from that list of measures and then the measure that you should take to mitigate that risk is also included, because it says no, we don't have MFA for example. What kind of risk does that bring with probability? But the impact is very high, we don't have MFA, the impact is also very high, because yes, we have a really weaker lock on the door. With guessing our password and even name they are inside, we have to score something more, but high and we will work on it and the measure is then and we implement MFA on the most important applications to start with, for example, so that process is often followed in that way, so that is what is done in basic or just based on a gut feeling. Advice, sometimes an assessment if an assessment or audit has been conducted. Yes, the recommendations that are contained in it, which are often risk-based, are adopted and those measures are then also implemented.

Q: Is that enough? Is enough being done to do this correctly?

Well, I don't think enough is being done to properly assess that risk, you know? So that whole risk management piece is still pretty immature. Taking measures to mitigate risks. I think a lot of work is being put into it, we're taking measures. We have to do this. We have to tighten this up, tighten that up. But it's still not enough. It's not being adequately assessed from a risk perspective, and it's more of a, well, we have to do this because we know it's not safe. Yeah, we also need to do something about awareness because that's really important. And, well, we have to make sure the system is as tight as possible. Something with authorization, so there's more of a focus on basic hygiene or basic measures that need to be taken, for example, written from a baseline level or, for example, what the NCSC calls the most important basic measures to prevent ransomware. And we're working on that. I think it's really good because then you really do set the bar a lot higher. But the additional piece would be: make sure you also continuously include it in your risk assessments and you'll actually see that you should always take those basic measures. But it might not be sufficient in certain situations and you still run quite a bit of risk if you don't do more than that in some areas. So I think risk management is still pretty immature. Taking measures and working to get information security underway. You can really see that a lot is being invested in that, but the same goes for it. Well, you only know if you're doing enough if you make those risk assessments on the front end, you know? So, yeah, I think that's the crux of it.

Monitoring and reviewing

23. Are the risks at housing associations evaluated and reviewed on a periodic basis? What should be periodic?

If it does happen, then I'm happy if they do it annually, you know? It should happen more often, you know? So I would, I would rather see it happen every six months or maybe even quarterly, to take another look and see if the risks have changed. Things change so fast, there are developments in the world that affect the risks you're taking. So I would actually recommend doing it quarterly. Yeah, you see it happen much less often, maybe even not for years, and that's not good. Like, the information security policy needs to be reevaluated. So, yeah, the plan-do-check-act cycle. I would recommend doing those planning activities at least once a year, with a risk analysis included. But, well, periodically reevaluating the risks together and seeing if they've changed, it doesn't have to be a very extensive review, but just in a small committee. Yeah, that's what I would do, I would do it more intensively than annually, so maybe twice or three times a year, and then I think it would be safe.

24. Are the risk assessment methods evaluated periodically at housing associations? If not, should this be done? And how could this be done best?

Well, that wouldn't be unreasonable. I often see that a methodology is used, a methodology is often used. I don't think it stops there. Like, we have to use this method, you know? If there is indeed a method being used, but what I just said is that often risks are really only thought of or inventoried in the front end. Yeah, you're sometimes helped based on a standard list to assess the chance of impact and eventually do something more with a business case or maybe even a business impact analysis (BIA) is sometimes done, you know? So the business impact analysis of the availability, integrity, confidentiality of your crown jewels, for example. But I think few questions are asked, is this methodology we're using here the best one and why do we choose this methodology in the first place? I think if the method is prescribed somewhere, it should be followed directly and no questions should be asked in the front end, and certainly not during the process either.

25. How can the periodic execution of the IT risk analysis be best ensured?

Yes, that it actually takes place. Yeah, you just have to implement your plan-do-check-act, because if you implement your plan-do-check-act, the risk analysis is automatically included, right? So it's automatically not. Of course, it has to be part of your planning, but there and also in your check, that's ultimately your risk analysis, but if you're going to implement it then. Then you'll include it and what does it mean to implement it? Well, you have to make sure you know what the process is that we're using here, who do we need for that, how often do we do it, and how do we make sure it happens? And who checks afterwards to see if we've actually done it? An ISMS (information security management system) can also help with that, right? By saying we're implementing an information security management system. To specifically record that. What do we do when? Who's involved in that? It's easier to hold someone responsible for an ISMS than to hold someone responsible for the entire information security, in which the process of information security is an important part. You can hold someone responsible for it, right? You have a man of an ISMS. You're not responsible for carrying out all the steps of the ISMS, but you do make

sure the system is implemented here and if the system is implemented, you have a structure with which you can work on information security annually through the plan-check-act cycle and where the risk analysis has its place. So I would actually advise doing that because then you have something to hold onto, you have a structure. You can also base it on a framework that you like to use, whether that's the ISO, the NIST, and work that way and make sure you go through your cycle with accountability on a yearly basis with your planning and have your agreements in place. At the end of the year, you know what we've done and everyone knows what we'll be doing next year and what is expected of those who have a role in the whole process."

Communication and consultation

26. In what form should the risks be best reported to management?

Yes, you probably have to do that very carefully. Well, you know. Report in clear and understandable language, focusing on the most important and largest risks. And then, yes, you just need to adequately involve them in that. Did you perform a risk analysis? There could be a very long list of those and it could also be a very long list with a lot of reds. Because we often do not fully comply at the beginning. But then you take the most important higher priority risks from that and focus on them and make choices based on them. And that is really the best management or board of directors here Our top 5 most important risks, for example, and we have to work on them and these measures are included in them, and you present it in a, well, a report or maybe even in a presentation form and that just continues to live and discuss it. I think that would be the right way to present those risks. The fact that you have to present those risks in this way perhaps says something about how you have carried out the risk analysis, because my suggestion would be to always give them such a prominent role in the entire risk analysis so that they are actually aware of what the largest risks are, right? So I would say, just start with a risk workshop at the front. Let's just think together. Yes, what are the risks now? What is the worst thing that could happen to us now? What is the biggest risk we are running now? What do you think of that and let them name some things and what you actually see is that they actually know it very well, but we have never written it down before. And if we do that today, we will write it down and then we will delve deeper into those risks, right? Going more in-depth into those risks, those are the risks. And what do they include? Then we will involve more people and we will think carefully about how we will assess and evaluate those risks and we will think carefully about what measures could be taken to mitigate those risks, and we will come back to you in a month. To be able to name the impact of certain risks more concretely, because that is the probability of those certain risks, but also what measures could be taken to mitigate those risks. And then the presentation they have is actually a feast of recognition. Because then they say, well, those are indeed the risks we mentioned. There may be some additional things added. Well, that is only good if we have more things than just what we thought of. And then there is actually also a plan to deal with those risks. So yes, I think that would be

the way not only to present them, but also to make them part of the process and therefore give them ownership.

27. Do housing associations often have an action plan / roadmap for mitigating identified risks? How could this look best?

    Yes, that is often included in a plan based on an ISO 27002. Those measures are listed. That's what you call sufficient yes or no? And no, then we will write it down and then we will do it, or we will comply to a certain extent in a certain way, and actually the column that you then fill in with. Well, those are not the measures that we need to take to comply with those standards often form a plan together and they are then. Based on priorities, often over time, refused to be carried out and this is how you have a year plan an IB plan. That will then be implemented, right? So we see that this is a method that is often used, therefore, from the risk and the policy document that lies in front of it. To develop a plan and implement it.

28. In your opinion, are the IT risks within housing associations sufficiently covered? Why or why not? What still needs to happen?

    You can't really give a definite answer on whether it is sufficiently covered. Because yes, that is different in every situation, right? What are those risks then, and maybe in some cases we see that they are sufficiently covered, in other situations they are not, and it also varies greatly again as to which risks are and are not sufficiently covered. But I think in general, if you ask the same question to housing associations, they really cannot answer that. And that actually says everything, I think, so then when we say, yes, can we say that now? Or actually, the question is, are you in control? Can you now say, am I in control of my control, in control of my IT or my information security, of my security, my privacy, in other words, yes, have we done enough to properly manage those risks now. Then the answer is, I think no one dares to say that. Yes, I don't know, or maybe not. And that really says enough. And then, well, therefore, if they cannot answer that, we don't want to say that it is too dramatic for sure, but the fact that you are not in control of that says enough, so I think that is the situation for most housing associations.

Privacy & information security within your organization

29. Are privacy & information security standards (ISO 27001, ISO 27002) currently being used in housing associations? If so, which ones? If not, would you recommend this?

    Already answered.

30. How can housing associations ensure that information is always available (availability)? Is this already being done well?

    I think in terms of availability, for the most part it is just, of course, also the story of outsourcing, right? And that may make the availability better than if they had it in-house, right? So there are of course a number of aspects, reasons why you say let a company that specializes in it do it. But doing it yourself, no longer placing the service here in a box and letting it run there. So I think in terms of availability, it is looked at in that way, right?

Saying yes, we have a lot of uptime, 99% uptime will be said. But if you look at what if we now have an incident. And. Yes, everything is still down, then it actually has nothing to do with the quality of performance or anything else, but you have to do with the quality of your security. That is actually not asked enough, right? So we actually see, you have a SLA, right? The service level agreements you have with a supplier. Actually mainly back. Yes, how do we guarantee that performance now? How do we guarantee that you have enough capacity, do you guarantee fast handling of questions and tickets from us, all focused on actually the service that feels like, yes, this is what it should be, right? This is the core, here it is about asking too few questions about how we ensure the same availability of those systems and therefore also of that data and often of our crown jewels when it comes to security aspects. What if we are now, well, or hit, or what do you actually do to prevent us from being hit, that attack surface, because that is what we are talking about in the end. Because a service provider is of course a large part of your attack surface as a housing association, right? How do we now reduce that and how do we ensure that the right measures are taken to make the chance of such a successful attack small and report once about it in your SLA. How many devices are there that we use that are not patched? How many incidents do you have per year? How is the monitoring arranged, are the backups securely safeguarded and do they also work when we need them later, all questions that are generally not asked, all very important for your availability, right? The availability of your information systems and therefore for your data, but where actually responsibility really lies with the one who is also responsible for it. The housing association to ask those questions to the supplier, but it happens too little.

31. How can the integrity of information within housing associations be properly ensured? In other words, how is the information protected against unauthorized or unusual modification or destruction? Is this already being done well

    Yes, that's what it's all about. Yes, how do we ensure that we are in control of everyone who has access to that data, that we know who they are? Well, a housing association often knows how to answer when it comes to its own internal organization, so we know about Pietje and Jantje and Joke who work here and who have access to those systems. And we often do think about how to make sure they don't have more access than necessary and how to make sure there is also a good lock on the door they come in through. But you also have suppliers who do things in those systems. You have admin rights, super admin rights and there is often a big risk there, so the integrity of your data depends on how many people can access it and what they do. How do we prevent unauthorized access to it? Because then you can never say whether it has been compromised or not. That piece of identity and access management, as it is nicely called, is also not well enough controlled and not enough thought has been given to the consequences of what happens if we have too many identities that have access and if we do not adequately secure access, we are really at risk in terms of the integrity of that data, because it could be stolen or

compromised. So yes, there is a big risk there, which I think is not adequately covered in the entire supply chain.

32. How can access to information be restricted to authorized persons within housing associations? In other words, how does the information remain confidential? Is this already being done well?

    You are responsible for it and also make choices for it. Nowadays, it's just about, does someone work within the organization and do they often have certain powers applied? So saying things like least privilege or anything else, we apply it, especially when it comes to systems that are sensitive in nature. Often you see that happening in the systems, but for example networks it happens less, but then of course it's just looked at per function. Yeah, what does each person need and how do we make sure they only get the data they need to do their job? So authorization matrix, etc. are really used. Yeah, it's checked periodically and logging is also checked, to see if anything weird is happening, and compliance is also monitored, but also outside the organization. So yeah, what can the supplier actually have now with full admin rights, and shouldn't they just ask permission before they get access to our systems before they do work that they absolutely need to do, because we rely on their services and know-how to keep the system up to date at our place. But yeah, we are in control when it comes to access to those systems and data in the systems, so ultimately it becomes risky when not enough questions are asked about it. It often goes reasonably well internally, but there is still a lot that can be improved. But there are many more actors who also have access, about which often no one knows and no questions are asked. And that's where it becomes risky.

33. How do housing associations comply with laws and regulations regarding privacy? For example, through compliance with the GDPR? Is this already being done well?

    Yes, taken into account, I think, and. I think that in 2018 it was quite a bit with the introduction of the General Data Protection Regulation (GDPR) that you then put the formalities, so to speak, in order and comply with those obligations. I think it is often in the processes themselves and in well, in everyday life maybe often not enough is taken into account. And you see different housing associations doing different things, right? So how do we protect privacy? But it often comes down to when something goes wrong and then action is taken. Like, okay, we should not do this anymore. Or should we do it? Or should we no longer record this kind of information? Or then you see that it is in the projects, for example, also the implementations of new systems, actually almost no questions are asked about? Well, We are now going to do a new, large-scale processing of data. Have I sufficiently weighed the privacy risks with a Data Protection Impact Assessment (DPIA), for example, can that be weighed? Yes, you hear that more often. But yes, I think that's something that really needed years and still needs to get that really in and that it is often seen as yes GDPR is a legal requirement and we check a box and we comply again. But that actually the underlying thought of okay, how are we going to make sure we embed it in all processes and take the right action never?

That that that that still often falls short, but you also see more and more improvements.

34. Are all actions within housing associations checked in the various information systems? (Auditability) and how is this done? Or how could this be done?

That is indeed a question that will differ per housing association and per system, but in general you can assume that logging is taking place, right? So that there is logging taking place on those systems and that the logging is also stored and secured in a safe way in case research needs to be done. But ideally, you would like to see that research is being done periodically or maybe even continuously on the basis of suspicious things or irregularities. And then you naturally need monitoring for that, right? But do all systems actually generate the log data that we want and do we know that and is it also done in the right way and do we know where that is and is it also usable and can we bring it together and can we do something with it in essence? Yes, those are questions that I think, I think not every housing association has answered yet. But well, you can assume that and then it becomes dangerous if you say that we assume that those systems are modern enough to generate that log information.

That is indeed a question that will vary per association per system, but generally you can assume that logging takes place, right? So that logging takes place on those systems and that it can also be securely stored and secured in case it needs to be investigated. But ideally, you would want there to be periodic or perhaps continuous investigation based on naturally suspicious activity to check for regularities. And of course, you need monitoring for that. But do all systems actually generate the log data we want and do we know that and is it also being done correctly? And do we know where it is and is it usable and can we bring it together and can we do something with it in essence? Yes, these are questions that not every corporation has answered. But it's dangerous to assume that those systems are modern enough to generate the logging information.

35. Are the information systems at housing associations regularly cleaned up? Irrelevant information removed?

I think not enough is happening. If we look specifically at compliance with the GDPR, perhaps the biggest risk and also the greatest. But yes. Difficulty is in practice. I think that many housing associations, so to the basic principle of the GDPR that you can no longer keep things, than strictly necessary plus that data that you do not need should not be kept at all. Yes, giving substance to those two basic principles is still difficult and that is also due to the whole legacy history of a housing association that they have built up a lot of data for years. And well, it's not easy to say goodbye to that. If it does succeed once, it is often a one-time thing. And yes, tomorrow you have created a new batch of data again. And how do you ensure that you clean it up periodically? Well, this is a, this is a challenge that many housing associations are dealing with, we also hear a lot about it. Yes, and there is not really a solution for it yet. You have a lot of fragmentary solutions for it. A lot also still comes down to the person

themselves to do it. In addition to the software area, there is more and more intelligence to be able to automate it. But yes, that In being in control overall, the holy grail is still not there. I haven't seen it yet in any case.

36. Is privacy and information security adequately safeguarded within the housing association sector? Why or why not?

Yes, I think, so yes, that is in line a bit with that story about the Plan-Do-Check-Act, because that is I think the way to ensure that you actually follow the plan-do-check-act and that you set a culture in which that succeeds. I think that some housing associations really have it together and know how to make it work. But yes, to keep it current and focused and not to let it become a yearly ritual and we check it off again and move on to the next year. Yes, you want to prevent that. It has to be meaningful and good. Yes, there are a lot of challenges for housing associations and it is also changing more and more and more is expected of people, so that yes, that part is very difficult. It often remains a one-time thing or maybe once in a while again, that policy, because that is now expired. Because we then linked an end date to it. We have to make new policy and then we pick it up again. Yes, then you do not ensure enough, I think, and you are not continuously, let's say, managing the risks, because that is what it ultimately comes down to. So I think that many housing associations do not succeed enough in that and that is not a criticism, but an observation and they also make that observation themselves. Yes, then you can do something with it, but I think that many housing associations also struggle with it. It is not easy. It requires human knowledge, it requires capacity. But yes, it is extremely important and vital for your service. So yes, you can not avoid it. And yes, giving it content is still the motto?

Expert interview 3

Your organisation in general

1. What is your position?

   I am the founder and partner at VVA Informatisering. An IT consulting firm, that is mainly active in the housing association sector, but also in healthcare, municipalities and education.

2. Are you also active in the housing association sector with your work?

   Definitely. From that perspective, I have been overseeing the eightfold hack since the very first moment of the report. From the moment an employee said, I didn't trust it until the co-writing of the final evaluation. Currently, we are in the phase where we are investigating the liability of the parties. I have been guiding the group of board members, business management managers, privacy officers, IT & security workers, and the communication group

3. If so, do you consider housing associations to be heavily dependent on IT systems?

   Yes definitely. The physical and digital worlds have become increasingly intertwined. This is particularly visible in (core) processes that are important for housing associations, such as housing allocation. In this process, people can register in a housing distribution system and, based on certain characteristics, such as registration period and urgency, qualify for scarce housing. Almost all housing associations have fully automated this process, although people can still go to the housing association for guidance in completing the application. Other processes, such as housing changes, where a housing inventory application is used and changes are automated and handled digitally. People can for example digitally sign for inventories and acceptance of housing, and repairs that still need to be done before leaving the housing can be recorded using a housing inventory app. The digitization of housing associations is therefore rapidly increasing and has taken off.

4. In your opinion, who should be responsible for:
   (a) Cybersecurity (securing your digital systems against digital threats)
   (b) IT risk management (all coordinated activities from the organization to steer and control IT risks)
   (c) Privacy & information security (ensuring the availability, integrity, confidentiality, privacy and auditability of information)
   There is a responsibility for information security and privacy within the organization that is carried out at every level, from management to the front-line employee. It is the responsibility of management to ensure that there is a clear and current information security policy and privacy policy. This policy-based part should also be updated by management and the executive team, strategically. At a tactical and strategic level, this means that risk management must be considered. If something happens, what processes should be most protected and what are our crown jewels? What measures do we want to take to deal with the risks,

what are the costs and what is our risk appetite? That should also happen at a tactical strategic level. Sits in-between tactical and strategic, I think. From a business operations perspective, it is also important to ensure that the privacy and security policy and risk management policy are adhered to. This should be continuously evaluated and adapted with the help of a damage circle. So on a tactical level, it must be overseen by a business operations manager that this process is also well set up and carried out and that the results are also followed up on. In addition, the organization has a privacy officer and a security officer who deal with the privacy and security policy. The security part is often delegated to the IT and Security responsible. If something happens, action must be taken quickly to limit the consequences and there must be a plan for the recovery of services.But the right agreements must also be made with the IT vendors, and the measures that are outsourced to third parties must be adequately addressed. You can't control it 100%, but you will still have to check it randomly or focus on the biggest risks from time to time. And look at whether a periodic backup can also be restored well. In case the data is ever stolen. Of course, there are also the end-users who need to be aware of their actions. What should be technically secure, right? Of course, you can't leave your laptop unchanged, you must run a privacy and security awareness program. That is also a responsibility at a tactical level, but rationally from employees on the floor, they should also participate in this and be aware of it. These are big issues and large security incidents are at least 70% caused by human action or have a major impact. So we can have everything policy-wise and technically set up, but if the human aspect is not given sufficient attention and safe actions, it can still go wrong.

5. Do you often see this as one function or are there often multiple roles within a function? Why do you think this is chosen? How would you like to see it?

   I doubt that the roles at housing associations are well-defined when it comes to privacy and security policy. In practice, I often see that the policy at the board level is not current and clear. The policy does exist, but is not well-maintained and the periodic risk assessment is often not done. From my experience with about 150 housing associations in the past 15 years, I have only come across a few that are truly actively managing IT risks. The role of the security officer has come to the fore after a hack, but was often neglected and not well-defined. The information and IT department is ultimately responsible for security, but there were often no clear tasks at the basis. On the field of awareness, I have seen that a lot of time and energy has been invested in recent years, especially by privacy officers and the IT department responsible.

   Cyber threats and your organisation

6. Have you ever worked with a housing association that has been a victim of a cyber attack? If so, what kind of attack?

Yes definitely, different types. There have been various types of fraud at this organization in the past. For example, there was fraudulent behavior by an employee who had access to the system and attempted fraud on his last day of work. Also, there was a hack of 8 housing associations at the end of March, and two weeks ago there was another housing association where the mailbox was stolen. This led to phishing attempts to have a payment account refunded, possibly as a prelude to further problems. Fortunately, it was noticed by an attentive employee that it was a phishing attempt, after which an investigation was started and it turned out that indeed a mailbox had been hacked.

7. And what has been the damage to the organization in question in terms of:
   (a) processes?
   (b) systems?
   (c) people?
   (d) finances?

Yes, what I see is that the last hack, which was the mailbox hack. You see that when we assessed the risk on Thursday evening, we determined that while it was just a mail hack, there was also a possibility that other systems had been hacked as well. The risk existed that there was access to primary systems and the document management system. At that moment, the only option was to disconnect all systems from the internet and network so that they could no longer be used by hackers. However, this also meant that employees could not work from Thursday evening until the weekend. To determine if there was indeed a network hack, we did forensic research over the weekend. Monday morning it appeared that it was safe to reconnect the systems and make them accessible to employees again. In this case, all systems were disconnected for about 1.5 days. So the mail could not be read, the phone central could not be reached, primary systems could not be accessed. Just really nothing. In this case, action was taken quickly and we also brought in external parties such as IT forensic specialists, lawyers and crisis communication experts to help us with the investigation and communication around the incident. We already had a incident response plan and it was discussed with the Board of Commissioners a week before. So when this incident occurred, we were well prepared and could act quickly.

Q: Is that something you see often with housing associations, that as a result of that hack in March, for example, that multiple people thought 'we should pay more attention to this' and set up an incident response plan or other things?

I think that prior to that, less than 5% of the associations had an up-to-date incident response plan on hand. I think now about half of the associations will have one, and that number is quickly increasing, so everyone has been made aware. If you look at the processes of the major hack where the systems were down for weeks. Normally, the recovery period would take about 3 weeks, but in this case, it took almost 9 months. Where it's not the case that they had no access to systems for 9 months, but rather 3 to 6 weeks occasionally or not. During that period, more and more systems were put back into use. The impact of the hack was enormous, as the

annual statement had to be approved by the accountant during that period. Questions had to be answered if the data being reviewed had not been manipulated by hackers. This made the process complicated and the rent increase that was pending, where all sorts of data is needed to carry that out. Yes, you miss a rent increase for a year, yes, then it runs for years and you'll be behind and that has cost organizations many millions. The primary process, such as reporting repair requests or closing payment arrangements, was also affected. Telephone switchboards and websites were sometimes down, so a emergency number had to be set up for contact. Everything had to be kept on paper and it had to be ensured that payments to contractors went through. It also had to be ensured that there was no fraud, such as submitting an invoice twice. The impact of the hack was enormous and especially for renters and employees.

8. Could this attack have been prevented? If so, how? Or what are the lessons learned?

   I can't tell you everything because it hasn't been officially published yet. Recently, there was a hack where multiple housing corporations were hacked, which was also in the news. The hack was successful by breaking into different customer environments. It is still being discussed how this could have happened. In general, it is important for parties to take maximum measures to prevent the situation from spreading to other customer environments. This can be achieved by having good authorization and monitoring and by quickly responding to unauthorized access to the system. The architecture of your network and signaling are very important. Although it's not always possible to prevent a hack, the consequences can be limited. This is also shown in reports of major hacks in the Netherlands, in which municipalities and schools, for example, have also been affected.

9. Is there a real threat of a cyber attack in the housing association sector in your opinion? Why?

   Yes, definitely. It seems that the public sector, including municipalities, educational institutions, and healthcare providers, are becoming increasingly targeted by hackers. Recently, there was a hack at Tragel, one of the major IT providers in healthcare, and several of their clients were affected by the consequences. Even the municipality of Antwerp was recently a victim of a hack. Commercial companies may be more inclined to pay a ransom to keep their hack out of the news. In the public sphere, they're a bit behind and are now working on developing incident response plans, monitoring the situation and performing "right to audit" towards their vendors to ensure everything is in order. It appears that the public and semi-public sector is a bit behind in terms of security, but they are now quickly catching up.

   Cybersecurity

10. Do the housing associations you have worked with use cybersecurity frameworks (such as NIST, ISO 27001, ISO 27002)? If so, which ones and why? Do you think housing associations should work with these frameworks?

The NEN 27.001 and two are ISO standards for information security that are often applied by providers of hosting or software products. Corporations are usually not certified, but there is a translation of these codes for information security (NEN 27001 27002) specifically for the housing association sector, called the "baseline information security corporations" (BIC). More and more housing corporations are also starting to look at the NIST framework for cybersecurity, because it is more focused on cyber vulnerabilities and how to prevent, detect and recover them. The NEN 27.001 and two focus more on taking measures and identifying critical processes and systems that need to be protected. Both frameworks help with structured thinking about information security and specifically managing cyber security risks and how to prevent them. And if it happens how to handle it best and how to address it in the future.

Q: Why would that shift take place? Is it because they are busy with that, because it explains something differently that gives me more?

Yes, it is more focused on cybersecurity vulnerabilities and what to do in case you are a victim or thinking in advance about some things that help in recovery, and also thinking more structurally about the risk profile that an organization runs, which is less relevant for NEN27001 and two. That is more focused on what measures have been taken. But it also goes more towards what are actually your crown jewels? Which processes are critical that have to continue? Which systems are critical that should not be out of the air? What data is critical. How do we ensure that data is properly stored and that we also regularly test if it could be restored in case of a disaster. So there is more attention to the risk assessment of information security. It also offers more tools for this, which has become more relevant in the context of more cyber attacks."

11. Do the housing associations you have worked with often have a cybersecurity specialist on staff? Why? If not, should they have a cybersecurity specialist on staff?

They don't have that in-house almost. Office automation has been outsourced more and more over the past 10 to 5 years, among other things because it has become technically too complicated. In the past, managing systems and networks was an MBO or MBO plus level, but now it is often HBO plus or even WO level, especially when it comes to the security aspect. This has led to the knowledge and skills being at higher and higher levels and the tasks becoming more specialized, including cyber security. This is often outsourced to parties who have scale benefits and can hire specialists who specifically focus on monitoring and interpreting monitoring tooling. This has led to the emergence of Security Operations Centers (SOC) solutions. For a medium-sized corporation or even one large corporation, this is often not feasible and that is still the case. More and more companies are working together with external parties to bring in extra expertise. Rates for this type of cyber security specialist have risen significantly, with rates between 175 and 350 euros per hour, often without additional charges for evenings and weekends. These are substantial amounts for a calamity.

12. How do housing associations stay informed about current cyber threats?

    I see that few housing associations actively research how the threat is evolving and what this means for the risk analysis that their organization does and the measures that are taken. Some associations have outsourced this to specialized parties, while others do join online forums or communities to stay informed. However, the majority seem to have no idea or have not actively paid attention to how the threat is evolving in terms of direction or speed.

13. Do you see many housing associations working together or seeking partnerships in the area of cybersecurity?

    It has been a common practice for a long time to work together within the housing corporation sector. The housing associations often have their own working areas, so they are not competitors with each other. Furthermore, there is often a shortage of housing, so housing associations do not see each other as competitors, especially not in areas where there is significant shrinkage. Instead, they work together to solve problems, such as large restructuring projects. Housing associations work together with a high degree of trust and share information with each other. In recent years, associations has increasingly focused on housing mediation. Through automated systems that have been set up together to keep costs affordable. Also in the field of ERP (Enterprise Resource Planning) regional cooperation was set up to establish an I&A management organization, because it is difficult to organize this individually and there are scale disadvantages. On the security front, we are also seeing more and more initiatives for regional cooperation, including by parties such as Corponet and Aedes. As these parties already cooperate in areas such as housing, ERP, and management organizations, they are also expanding their cooperation in this theme.

14. Are the housing associations you have been at sufficiently secure against a cyber attack? Why or why not? What still needs to happen?

    The risk analysis is very important to do at the beginning, because it is an almost unexplored area that is also focused on by NIST and your research. It may not even be in its infancy yet. Therefore, it is important to pick this up quickly and determine what we need to secure, how we should secure it, and at what cost. Once these questions have been answered, we can move on to operationalizing and making sure that this becomes a cyclical process that is updated periodically or at least on a quarterly basis. So, embedding that whole risk thinking and also the execution of it and the monitoring and the cyclic-making of the whole policy from risk appetite to measures to execution of it and monitoring. This is something that will have to be heavily invested in. Good cyber incident response plans should also be in place and the organization should be prepared for these types of situations so that we can act quickly and adequately on a technical, communication and stakeholder management level, as well as legal, reporting to the police, to the AP. The goal is to keep the consequences of an incident as small as possible with the help of monitoring and other

means. There is still a lot of work to do on the whole spectrum of this process.

IT risk management and your organization

Context establishment

15. Is there a formalized (IT) risk management policy at the housing associations you have been at? And when does this date from?

    Housing associations are fairly active in regularly checking their compliance with standards such as the Baseline Informatiebeveiliging Corporatie (BIC) and NEN 27.001. They look at whether they have taken the minimum measures and if so, to what extent, and if not, what will they do about it. This happens quite often and periodically, but in many housing associations it can happen that it has been 2-5 years since it was last looked at. A policy document was prepared and security plans based on a framework. These plans usually have a implementation period of one or a few years. However, there is still little active monitoring of the location of crown jewels such as crucial processes, systems and data, and the risks that occur. Risk assessment is also rarely done. To give an idea, in recent years phishing has increased enormously and has affected many vulnerable organizations. This is why two- or multifactor authentication is now being used more and more. The market is not standing still, now there is also increasingly talk of smishing, in which security incidents are provoked via SMS messages instead of e-mails. Fewer people are familiar with this. Hackers are developing and more and more attacks are being made via social media and artificial intelligence is being used for attacks. It is therefore important to stay informed of the latest threats and to take extra measures to protect the organization.

16. How is the risk acceptance level (risk appetite) determined in housing associations, and by whom?

    However, it is often the case that dialogue about risk appetite is insufficient, both qualitatively and quantitatively, which can cause problems. Risk appetite assumes that you already have a clear understanding of the risks, which is often not the case. A NIST (National Institute of Standards and Technology) framework can help to have a structured view of risks and to take measures to reduce them. Risk management does take place within housing associations but less so in IT. If this were to take place, it would be a good step forward. Then you would at least have an overview of where the risks are, you would have an understanding of the value, how great the impact is and where it is located. And then you can actually start looking at what measures can be taken to make those risks smaller and to make the impact smaller? And yes, what measures are associated with it and what does it cost? So you actually need all those steps to come to a decision. A cyber security specialist, internal or external, can support this by indicating where the risks are and together with the business weighing the impact in the decisions. The decisions about risk appetite, the costs, what am I going to mitigate? That is a tactical strategic question that is decided at the executive level. Fed by the people and ingredients discussed earlier.

17. How are IT risks classified, prioritized, and mitigated (processes to reduce the negative consequences of risks)? What measures can be taken or need to be taken for this? And is enough being done within housing associations to properly regulate this?

    In general, risk management within housing associations, which is the majority of housing associations, I think the percentage is between 80% and 90%, are actively managing risks in various areas. This can be done, for example, using risk management systems that are kept in Excel. One of the biggest risks that housing associations may face is a decline in the property market. If the value of real estate drops drastically, this can affect the equity or tax part of a housing association of 20,000 homes, which can quickly be a billion. This in turn can affect the borrowing capacity of the housing association and the new construction projects that can be carried out. Therefore, these risks are continuously managed, as well as land positions and other things.

    Q: And more specific IT risks?

    In the 20 years that I have worked in the housing association sector, I have only once been asked to periodically describe IT risks as well. This involved questions such as what happens if a system fails or automation no longer works, or what it means if a primary system fails. Although hacking a system was hardly considered at the time, it is now a real risk that housing associations need to take into account.

18. How should risk assessments (assessment) take place within a housing association?

    The hack that occurred at the end of March has led many organizations to focus on creating incident response plans and conducting a business impact analysis to determine the risks they face. They are also doing risk assessments. They are keeping a close eye on how they are doing, but not necessarily looking at what is happening in the market. The goal is to map out the impact on processes, systems, and data if they are affected. It has had a cascading effect as a result of the hack.

19. Are the risks at housing associations evaluated and reviewed on a periodic basis? What should be periodic?

    It starts with the fact that they have to be reviewed in the first place, and that there is awareness of this. I'm sure that there are now many corporations that say that they are going to take a look at their systems, processes and data once, but that has to be done regularly. It is especially important to periodically look at the systems, processes and data of a association, because the processes are increasingly automated and the impact of a hack in this case would be greater than before. This applies, for example, to the housing intake process, which takes place entirely digitally, and to the tradesmen of a association who no longer have to go to the office to pick up their work orders, because everything is digital. When this is not done, it's back to basics again. It's also important to keep looking at whether the existing risks are still the same or whether there are new or weakened risks. There is a kind of quarterly cycle that must come

back at least, and that the organizations will have to create feelers to stay informed about how the threat develops in terms of pace and direction. This is almost impossible for a association to do individually and it is therefore necessary to seek help from parties that can do this for or with the association.

Communication and consultation

20. In what form should the risks be best reported to management?

When you have a risk management information system, such as Excel or a more advanced system, you often see a traffic light method. This occurs when a new risk arises or when the weighting of an existing risk changes, for example from green to orange or vice versa. This method is useful because it can quickly help to identify changes in risks that require additional attention. As an organization, you often have many risks to manage, such as rent arrears and vacancies. It is therefore important to manage these risks with a traffic light method, so that you can keep an overview and be prepared for any changes that require additional explanation. This is how, in my opinion, risk management should be done within an organization.

21. Do housing associations often have an action plan / roadmap for mitigating identified risks? How could this look best?

A certain structure has been put in place for the risk management system. The corporate controller is often responsible for this process and ensures that risks receive the necessary attention and that there is a logical flow and continuity in place.

Q: Once risks have been identified, is there often an action plan made to mitigate them?

There is regular meetings with the management team and board members to discuss overall risk management. However, creating a roadmap on how to handle situations and implement measures is dependent on the specific risk at hand and requires specialized expertise. To assess and propose measures for specific risks, the right people need to be gathered. It is the responsibility of the chief financial officer for this process.

22. In your opinion, are the IT risks within housing associations sufficiently covered? Why or why not? What still needs to happen?

I believe that the most important thing is that associations and organizations in general must realize that taking on a software system or fully outsourcing office automation to an external party does not mean that they no longer have a responsibility to oversee these systems. This used to be a line of thinking, but it is important to realize that responsibility does not end as soon as something is outsourced. It is therefore recommended to perform periodic audits or penetration tests and set up independent monitoring to check if the measures of the external party are actually being carried out. It's also important to look at authorization and multi-factor authentication from the supplier's management perspective, so that unauthorized people cannot gain access

to the system. Awareness will continue to be extremely important. It remains important to take into account the risk of human error and to have a plan to keep the effects of a hack as small as possible. These issues deserve attention and will continue to be important in the coming period.

Privacy & information security within your organization

23. Are privacy & information security standards (ISO 27001, ISO 27002) currently being used in housing associations? If so, which ones? If not, would you recommend this?

    It is correct, and what you increasingly see is that more demands are being made on suppliers to have an ISAE 3402 TYPE 1 statement, which shows that they have secured their processes. But there are also TYPE 2 statements that ensure that attention is paid to the application of security processes. These processes are often focused on obtaining financial security, for example by applying information security measures to verify the reliability of financial systems. Supervisors are also increasingly ensuring the rise of ISAE 34 TYPE 2. However, it is important to note that having these certifications does not necessarily mean that a company is completely secure and there have been cases where companies that have these certifications have still been hacked. Furthermore, the General Data Protection Regulation, or GDPR, is also simply a privacy law that everyone must comply with.

24. How can housing associations ensure that information is always available (availability)? Is this already being done well?

    Often it is outsourced, and typically a SLA (Service Level Agreement) or Processing Agreement is established in which suppliers take on certain uptime guarantees and take appropriate measures to ensure the availability of a system.

25. How can the integrity of information within housing associations be properly ensured? In other words, how is the information protected against unauthorized or unusual modification or destruction? Is this already being done well?

    It really depends on which aspect you are looking at. For example, when looking at a system from the scope of a procurement process, corporations often ask for the ability to log data from the system, so that transactions can be tracked over time and any fraudulent activities can be detected. Additionally, requirements are set for multi-factor authentication and authorization, so that only authorized individuals have access to certain data. That is on the authentication side, but also you have the possibilities you have for authorization that people can only see what they need, but not more than that. You also see a change in that, in the past, a context-dependent approach was often chosen, where all authorizations were opened so that employees had a complete picture of a tenant's situation. Nowadays, however, a role and rights-based approach is increasingly being chosen, where only the authorizations are given that are necessary to perform a specific task. This has the advantage that there is less risk of unauthorized access to data. But yes, with the current privacy

legislation with data access authorization, someone is only allowed to see what is actually necessary for you. Not more than that, you see that there are many more barriers between data within systems.

26. How do housing associations comply with laws and regulations regarding privacy? For example, through compliance with the GDPR? Is this already being done well?

    The framework of the General Data Protection Regulation (GDPR) cannot be avoided. On the one hand, it's a hygiene factor, but on the other hand, there are associations that also see it as a way to be reliable and do good business, not just because it is required by law. They also see it as their responsibility to ensure that everything is properly arranged for dependent parties, as well as for employees and other stakeholders with whom they share information and data.

27. Are all actions within housing associations checked in the various information systems? (Auditability) and how is this done? Or how could this be done?

    It is very rare that associations look at their logging data, more than 95% and maybe even 98% do not do this or do it very little. This only happens when there is a reason, for example if there are suspicions of fraud. For example, in the housing allocation system, looking at the last 30 homes that had gone away in the past six months and that had all had an adjustment in the registration period that had been modified by John or Jack. This kind of thing also happens and can be found in the newspaper, such as at Thuisvester where an investigation was conducted into someone who favored others in the housing allocation system and was reportedly also paid for it. When this kind of thing happens again, you sometimes see a resurgence of interest in looking at the data, while it should actually be standard to check when adjustments are made to the registration period of a housing seeker. This should immediately set off all alarm bells, unless the person in question has obtained extra urgency in a special situation, which is then understandable. However, in most systems, there is no monitoring logic that checks for this type of triggers.

28. Are the information systems at housing associations regularly cleaned up? Irrelevant information removed?

    Yes, there are legal retention periods, which must also be followed by associations. Some document management systems (DMS) provide good support for this by, for example, asking to indicate what the standard retention period is for a certain document. Other systems, however, do not have these types of mechanisms, so it is up to associations to conduct periodic checks and delete data. Sometimes this is not possible because the system does not allow it or because deleting certain data causes problems. Many organizations are also not actively engaged in managing their retention periods. That's why we offer a service to clean up and scan the network for personal data that may no longer be stored according to the GDPR, such as ID cards, passports and certificates of good conduct. However, many associations have not yet performed scans of this kind of data, so there is still a lot to gain or room for improvement.

29. Is privacy and information security adequately safeguarded within the housing association sector? Why or why not?

    I think the text is a summary of the sub-answers given during the interview. Policy-wise, it should be clear, so what I said at the beginning needs to be reviewed and updated periodically. This applies to risk analysis, business impact analysis, and determining measures to mitigate or accept risks. It's also important to have good implementation of risk management and to apply it periodically. It's also important to keep an outside view on direction and speed developments. It's also important to keep employees aware and for the organization to stay informed about the latest developments in the field of events.

Expert interview 4

1. What is your position?

   I am the director and owner of a BV, which is an advertising agency, photo studio, and video company.

2. Who should be responsible for:
   (a) Cybersecurity?
   The board. I always find that the management or board often don't feel that way and don't experience it as such. That's also where part of the cyber problem becomes apparent.
   Q: Why do you think that they don't experience it as such?
   Because they have the practical evidence that cyber is not a concern, as those companies have existed for 10, 20, 50, 100 years and have never been hacked. So you can see that it's not a problem, and that's exactly the problem.
   (b) IT risk management?
   Companies with 25 or more employees often already have their own IT department with specialists to manage IT matters. However, it can be more difficult for smaller businesses and freelancers to have someone who deals with digital matters. Therefore, I think it would be a good idea if every company with 1 to 10 employees had a digital helper (DHV), someone who is interested in IT matters and who gets a few hours per week for this. This person can check strange emails, contact IT companies, and report to management, just like a business helper (BHV) does but in the digital field. This would help ensure that small businesses are better protected against digital threats.
   (c) Privacy & information security?
   I think that can only be the management. The management is always responsible and IT professionals only look at the technical part. The part on the human resources side, that is often not there, but if it is, they often look at the substantive part of what data we have from people. The security of the data, I think that is primarily the concern of the management.

3. Do you often see this as one function or are there often multiple roles within a function? Why do you think this is chosen? How would you like to see it?

   What I usually see is that the roles are not assigned and that there is really no one who is truly responsible. In smaller SMEs, there is no one really responsible for the problem. That's exactly the problem and in larger organizations, it really depends on how big you go. For example, I work for Nutricia Danone, they really have it all together and it's really tight.

   Q: How should smaller organizations take care of this?

   Cybersecurity is important for all companies, regardless of their size or scope. Smaller businesses may tend to underestimate the danger of cyber attacks because they do not see themselves as an attractive target. However, it is important to realize that it is not just about the individual

company, but about the entire supply chain. If a small business is a weak link in the chain, it can be dangerous for the larger parties it works with. Therefore, it is important for smaller businesses to also get their cybersecurity in order and to appoint someone to take care of it. This way, they can be a safer chain partner and reduce the risk of a supply chain attack.

Cyber threats and your organisation

4. Victim of cyber attack?

   Yes, a brute force attack.

   Q: What is a brute force attack?

   Someone from the outside can log in to our server, such as a part-timer or someone working from home. This can be done with a username and password. With a brute force attack, they don't know for sure if they have the correct username and password. They try to guess the password with 1000 attempts per second, just like you used to try to open a combination lock when you forgot the code. It took us 4.5 hours before they succeeded. According to calculations, it should actually take 8 hours to guess our password, based on the ratio between the password and the time it takes to guess it. But technology has improved greatly and the data traffic through fiber optics has increased enormously. So according to the table for 2022, it would now only take 39 minutes to guess our password. Technology and computers have accelerated spectacularly

   Q: So the threat is increasing?

   Both the threat and the importance of getting your security in order are increasing. Hacking a password of 8 characters takes almost zero seconds nowadays.

5. And what has been the damage to the organization in question in terms of:
   (a) finances?
   Primary damage, 1/4 million to repair. 4 months later, another 1/4 million. 10 months later, another 1/4 million. And 18 months later, the total was 1.5 million. And then I had to declare bankruptcy for the company.
   (b) And what about processes, people and the organization?
   It is very important to understand that the initial damage of the cyber attack, approximately 250,000 euros, is survivable. But the consequential damage, such as the impact on staff, the impact on customers, the stopping of orders, the reduction of requests for quotes and damage claims, is almost not survivable. If your business depends on digital data, such as photos, videos, and graphic work, the image damage resulting from a hack is almost not survivable. If you are, for example, a violinist on a terrace at a restaurant, it is not so bad if you are hacked because you can play the next evening and earn money again. But for SMEs, the consequential damage is six times greater than the initial damage. For the municipality of Hof van Twente, which was also hacked,

the consequential damage is even 20 times greater than the initial damage and is still increasing.

6. Could this attack have been prevented? If so, how?

   That could have been prevented with a better password. SMEs don't know what a good password is. I think if I don't know it, I think it's a good password. But it's mainly about the length of the password. It should be at least 15 characters, preferably longer, preferably with a password phrase or password manager. And MFA should be turned on. If we had those two things on, the hack would not have happened.

7. What are the other lessons learned?

   Digital basic hygiene must be in order. Like the seatbelt in your car, which everyone thinks is normal, you have to have these basic things in order. However, SMEs in the Netherlands do not have this in order. Really not. Those are the lessons learned.

8. Is there a real threat of a cyber attack in the housing association sector in your opinion? Why?

   The number of cyber attacks is increasing exponentially, for various reasons. There are large groups of hackers who organize in communities, and some just collect data and trade email addresses and passwords in databases. There are now 3.2 billion email addresses and passwords for sale. These are sold to an increasing number of hacker communities that use ransomware software, and these attacks quadruple annually because there is so much money to be made in such an easy way. Companies with multiple employees, such as hospitals, schools, and housing corporations, run an increased risk of someone clicking on a phishing email and becoming a victim. In addition, there are also state hackers who are out to disrupt our society. This is also the reason why municipalities and housing corporations are attacked. If these hackers can hack and send messages about double rents, write-downs, evictions, for example, some governments can use this to distract attention from conflicts in Russia and Ukraine, for example.

   Cybersecurity

9. Do the housing associations you have worked with use cybersecurity frameworks (such as NIST, ISO 27001, ISO 27002)? If so, which ones and why? Do you think housing associations should work with these frameworks?

   It is indeed true that some frameworks, such as ISO certification, are good for capturing processes in an organization, but they do not guarantee that they will also be followed. This is because it is individual employees who ultimately perform actions, and it is important that they are competent and know what they need to do to reduce cyber risks. I am building an e-learning platform to help people in different sectors understand what the risks are and how to deal with them. This can certainly help to increase the awareness and competence of individual employees, which in turn can contribute to a safer cyber space for everyone. Finally, I think the

frameworks are good, but they are still not enough for smaller businesses. For small businesses, they are impractical.

10. Do the housing associations you have worked with often have a cybersecurity specialist on staff? Why? If not, should they have a cybersecurity specialist on staff?

    No, I don't see that. You do have CISO's [Chief Information Security Officer] often. It is the case that companies with many employees, such as municipalities and large associations, often have to deflect thousands of attacks per day and try to keep their employees aware of the risks of downloading apps and taking WiFi-sensitive equipment to work. Additionally, it remains a challenge for IT departments, which often have to work to keep up with the knowledge needed to maintain security. Often, this specialized knowledge is not in-house.

11. Do housing associations often receive support in the area of cybersecurity? If so, from whom? If not, do housing associations need support? Why?

    If you ask where they should get it from, I would say they should find it themselves. Entrepreneurs should be entrepreneurs and not depend on others. In the case of housing associations, I think it is important for their IT departments to work together in weekly meetings, like we do here. This way, they can identify threats and share information about current problems. If they do this, they can hire a cyber specialist to help with the solution and share that knowledge as well. That is how entrepreneurship should be. We need to talk to each other and work together to achieve spectacular improvements, but everyone seems to be so entrenched in their own tunnel that they don't do it.

    Q: So cooperation is needed in the sector?

    It is essential to survive, because it's going too fast. It's too innovative. Hackers have unlimited resources and unlimited patience. In the past, a burglar might climb over someone's fence and you'd have to kick them out. Now, it's just thousands of people climbing over the fence every day. It's not practical for a business owner to say, 'Yes, I'll do it alone. Yes, I'm not an expert and I'll just do it as a side thing.' That's not a strategy for coping with this.

12. How could your organization stay even better informed about current cyber threats? How could housing associations stay informed about current cyber threats?

    There are some platforms that do a good job for the Digital Trust Center, such as the website of Economic Affairs. Cybercrime Info is also an excellent website, founded by cyber specialist Peter Lahousse from Breda. This website is managed by the national police and offers weekly updates and newsletters about all cyber threats. It is free and there is a lot of useful information to be found, but for housing associations it is different because they have a completely different risk profile. This means that as specialists you need to look at the specific risks that apply to them, such as when rent increases take place. If these cannot be implemented due to a hack, this could lead to a loss of 4% of the rent to be collected. Hackers are often

already inside and have already bought login details from other hackers to look at the risk profile of housing associations. They can then decide when to carry out a ransomware attack, or sell the obtained data to other hackers who use ransomware. It is important to talk to your own sector about the specific risks and not just focus on what you can do against ransomware.

IT risk management and your organization

13. Do the housing associations you have been at use a risk management standard (risk management norms, describe processes and are intended to identify and limit risks)? If so, which ones?

    Who can dictate this for the housing corporation sector? I am an outsider. Who can do this better than the sector itself? Set up a consultation and bring those risks to light. Are there risks in August? Are there risks in January? You as a sector need to think about that, think about it together and develop a plan together. Find out what the risk profile is and then you can easily go to a cyber specialist like a FOX IT or a data expert or an ethical hacker to see what measures we need? You don't need to do all of that individually, preferably not. Do that together to get a good overview of all the vulnerabilities. There are a lot of vulnerabilities.

    Risk identification, Risk analysis, Risk Evaluation (Risk assessment)

14. How are IT risks identified in the housing associations you have been at?

    his should be done by the housing association itself. People who are responsible within the housing association should be responsible for inventorying that for us and discussing it with the others so that we can come to that risk profile together.

15. How and with what frequency should these risks be evaluated?

    Things move very fast in the cyber world. I would say start with a biweekly consultation. Also, conduct a penetration test twice a year or perhaps even four times a year. Or instead of a pen test, invite an ethical hacker to carry out attacks to see if your organization is in order.

    Q: And what should they discuss in the biweekly consultation?

    There are a number of things to consider when it comes to protecting against hackers. For example, it is important to share experiences and create lists of attention points and potential concerns and vulnerabilities, and the solutions for them. We also need to take into account the fact that every employee within the housing association already has 50 to 60 apps on their phone that are easily hackable. And I haven't even mentioned the organizations or websites or apps or systems of the housing association itself yet. But if we already have 60 ways to get in through the staff, we are a "sitting duck" or "fish in a barrel", meaning we are easily hackable. This is not only a concern for the housing association, but also for other organizations. For example, a hackers community was recently hacked by another group of hackers, in which there was 2.4 billion dollars on the bank account. This shows that hackers have unlimited resources to carry out attacks, so we must not underestimate our naivety and think that a good password will always protect us.

16. Are risks in housing associations classified in a standardized way (chance * impact)? If not, should this be done?

    The chance that something will happen once and the impact it would have is a very theoretical approach that I quickly do not believe is the way to go. It is never possible to completely eliminate the chance of being hacked. In my opinion, the chance is about 1 in 5 that you will be hacked. If you are hacked, you must also consider the impact of the hack. The impact is about 5 times the chance of being hacked, and the damage is about 6 times the impact. But we must also realize that the financial damage is not the only thing to consider. In our financial society we often only look at money, but we must also look at what the hack does to you and your people. This can lead to burnouts, overstrain, disability, rising health costs and absenteeism, which can be much more expensive in the long run than the financial damage. Money is endlessly circulated, but the real damage is in the effects on you and your people.

    Monitoring and reviewing

17. Are the risks at housing associations evaluated and reviewed on a periodic basis? What should be periodic?

    Consult with IT guys, guest speakers, ethical hackers, cyber specialists and I think evaluate quarterly so 4 times a year. I think that is enough for now.

18. Are the risk assessment methods evaluated periodically at housing associations? If not, should this be done? And how could this be done best?

    These risks are clearly present and must be addressed. There must be budget to reduce these risks and there must be support from the board and management to put this on the agenda. It is essential to take these threats seriously and actively address them, so that we are not just watching them happen. As an IT professional, it is important to raise this and emphasize how important it is to be actively involved in this, but it is also important to emphasize that it is not just up to you to solve the problem. It is important that everyone in the organization takes ownership and is aware of these threats and how they can be addressed.

19. How can the periodic execution of the IT risk analysis be best ensured?

    For small SMEs with 20 people, I would say: Do it with the DHV, the digital helper, who produces a report to the management every quarter or in the work meeting. That the DHV has one hour in the work meeting every three months to explain the status. In larger organizations, this must be more formalized in other consultation structures.

    Communication and consultation

20. In what form should the risks be best reported to management?

    In personal consultation and not in reports. For example, I am good at taking photos and videos and therefore started this company. Although I am part of the management, I have no knowledge of cyber. When I receive a report on cyber, I have difficulty reading it and often do not understand it because I am busy and cannot assess the risks. That is why it is important

to discuss these things on a personal level so that we can understand each other and solve the problem. This can be done, for example, by purchasing specific equipment or hiring a hacker or pen-tester. It is not only important to create awareness, but also to adapt the company culture so that problems can be easily discussed. If, for example, Jannie receives a suspicious email, she should be able to easily call Henk for help. Henk, as DHV or department head, can then report to the IT department or the CISO and ask for measures to be taken against this type of spam, phishing or spoofing. In this way, the problem can be effectively addressed. It is important to change the company culture so that Jannie knows where to go if such situations arise. It is also important to make these things discussable so that we can communicate and solve problems effectively.

I find it strange that there is a sign at the housing association's coffee machine with instructions in case of fire, while the chance of fire is only 1 in 8000 and the average damage is €14,000, while there is no cyber plan in case of cyber, where the chance is 1 in 5 and the average damage is €340,000. If you receive a suspicious email or have clicked on something, call the DHV. I am happy if I can call Henk if I receive such an email or have clicked on something, because then I know that there is someone who can help me solve the problem.

21. In your opinion, are the IT risks within housing associations sufficiently covered? Why or why not? What still needs to happen?

I think it's important to realize that technology only plays a small role in cyber security. It's actually only about a third of what it means. Another important factor is the leadership and decision-making of management and leadership. They must ensure that cyber security remains on the agenda and that funds are allocated to address it. Another third factor is the behavior and culture of people on the floor. We often tend as managers to have people click on everything that comes by, which actually creates risks. If something goes wrong, we blame the employees. But it's also up to us to ensure that they are protected against wrong clicks, for example by using catch nets. So technology is only a small part of cyber security, despite thinking that antivirus software and firewalls solve everything. In reality, antivirus software only keeps 54% of viruses and malware, while 30,000 new viruses come out every day. So it's a challenge to keep everything in order.

Privacy & information security within your organization

22. How can housing associations ensure that information is always available (availability)? Is this already being done well?

It is not possible to guarantee that your data will never be lost and will always be accessible. However, by working with backups and storing data in multiple locations, you can ensure that you can restore the data after a short downtime. However, the more locations you use to store data, the more vulnerabilities you also create. There is always the risk that one of those locations will be hacked.

23. How can the integrity of information within housing associations be properly ensured? In other words, how is the information protected against unauthorized or unusual modification or destruction? Is this already being done well?

    Storing data in various silos and encrypting it is a good way to secure the data. It adds an extra layer of security because hackers are unable to access all the silos at the same time. It is also a good idea to use multifactor authentication (MFA) to ensure that only authorized individuals have access to the data. It is important to realize, however, that there is always a risk that the data may be lost or become inaccessible in some way. Therefore, it is recommended to regularly create backups and store them in multiple locations. This way, the data can be quickly restored if something happens to one of the silos or if some other incident occurs.

24. How do housing associations comply with laws and regulations regarding privacy? For example, through compliance with the GDPR? Is this already being done well?

    There is a lot of blind trust among businesses. I work for about 30 municipalities and the municipality I work for has it well organized and is very cautious. But with other businesses, I often see that they simply trust someone to make sure everything is in order, such as the PO (Privacy Officer). Meanwhile, they use the information themselves in an irresponsible manner because they do not feel responsible. For example, they might think: "I'll just send the entire staff list for the Christmas card. Can I do that? Yeah, I think so. I have access, so it must be okay." But that is not correct.

25. Are all actions within housing associations checked in the various information systems? (Auditability) and how is this done? Or how could this be done?

    From what I see, it is the CISOs who do this. And the CISOs are the ones who face a lot of resistance in the team because they are perceived as being difficult and disruptive. But I'm busy and I just need to know what's going on. I need this, it's not that difficult to do. The reason for this is that some corporate cultures are not yet mature enough for this matter. There needs to be more discussion on this topic and more understanding needs to be developed.

26. Are the information systems at housing associations regularly cleaned up? Irrelevant information removed?

    Yes, you can see that well with Forum for Democracy. I think that is a prime example of how it is easily regulated. We need an app, we need this, we need that. And for the rest I don't really know either. It is more the exception than the rule.

27. Is privacy and information security adequately safeguarded within the housing association sector? Why or why not? Or are improvements needed in all of the above aspects? If so, which ones? Why?

There are communities of hackers who are only interested in personal data for social engineering. They try to obtain those profiles and sell them for around €20 per profile, depending on how complete it is and whether, for example, a passport or BSN number is included. This is an emerging industry, not to hack, but to trade data with various parties. It is an increasingly greater threat to be hacked, because your profile is becoming more valuable and is being traded more. There can be up to 3 years between the collection of data via phishing or other methods and the actual hack. There is often insufficient understanding that your data is being traded, which can result in, for example, 10 hackers coming to your door. These kinds of mechanisms need attention and we really need to talk about them.

Expert interview 5

Your organisation in general

1. What is your position? And what kind of organization do you work for?

   My name is Olaf van Dijk and I am a member of the executive team of Zich Web Software. We've been building web applications since 1999, with a specific focus on housing associations since 2001. I have a background in business economics and studied at VU, where I took all IT courses that are closely related to business informatics. I've been a member of the executive team since 2006, and within that team, I am responsible for operations and professional services. Additionally, since 2004, I've been working with information security and have the role of CISO (Chief Information Security Officer).

2. Are you also active in the housing association sector with your work?

   We primarily make software for the life of the housing associations that we serve. These are what we call the "Front Office" applications, which means they are focused on the customer interface. Within housing associations, there are also back-office systems, such as the "System of Records" where a lot of storage, financial processing, and other back-office functionality takes place. However, our applications are focused on customer interaction and also have a piece of back-office functionality for the housing corporation employees. Our software is used by approximately 200 associations in the Netherlands.

3. Do you consider housing associations to be heavily dependent on IT systems?

   Increasingly, the administrative processes of housing corporations are automated and running on decoupled systems, such as expert systems on various fronts. This is a result of the digital transformation taking place in various industries, including insurance, government, and municipalities, and now also at housing associations. The transition from heavy administrative back-office systems to decoupled systems has also been experienced, particularly around 2002-2004. At the beginning of the century, this was much less and differently shaped. The growth of automated processes has been fast in recent years and is expected to continue.

4. In your opinion, who should be responsible for:
   (a) Cybersecurity (securing your digital systems against digital threats)
   Security and awareness are an important aspect of digital systems and IT systems for housing associations. Security awareness, according to my experience, has increased since 2004, though it can still be difficult to handle the complexity of application and functional management within the organization itself. This is particularly the case for smaller associations with 50 to 100 employees, who often struggle to keep expertise on board. As a result, a large portion of IT and applications is outsourced, with the corporation employees often working at a user level. While it has improved in recent years, it is still challenging to find people with

expertise in application and functional management. There is a need for this.

(b) IT risk management (all coordinated activities from the organization to steer and control IT risks)
Yes, organization-wide, that is the case with every organization. Awareness of this needs to be present at all levels, especially at the executive level, because the organization is financially responsible for a large portion of its assets. This is particularly the case for housing associations that are mainly focused on real estate and investments in bricks and maintenance. But IT is also important and some larger organizations understand that. However, it remains a challenge for organizations such as healthcare and government institutions, where primary tasks are less focused on digital technology. This also applies to banks and insurance companies, which used to be offices with people behind counters and glass walls, but now are fully digitized and process an enormous amount of data. The IT component is becoming increasingly important for housing associations, especially for the administrative side of bricks and mortar properties.

(c) Privacy & information security (ensuring the availability, integrity, confidentiality, privacy and auditability of information)
Traditionally, IT often comes from a financial angle, with an executive who also has financial matters in their portfolio. It is best if the functional management of an application is built out of a mix of IT-related people and people from the business, such as people from rental and housing affairs who can act as knowledgeable users or key users.

5. Do you often see this as one function or are there often multiple roles within a function? Why do you think this is chosen? How would you like to see it?

   Housing associations often struggle with appointing a privacy officer, who is often only appointed in case of emergencies and is not involved in daily operations. This also applies to other organizations that often hire interim staff for a short time to complete a specific task, without it being embedded in the organization. It is a complex role that requires the person to be well-versed in both IT and business processes and have a sense of developments on both business and technical fronts. My vision is that it would be better if there were more business owners for applications instead of IT departments, so that the business is also responsible for the application and able to set requirements. This may also mean hiring experts from outside, but the business must be involved in the conversation about security and improving it. When it comes to legal matters, some organizations send an IT lawyer who is good at legal matters but doesn't understand the underlying IT landscape. Or there are IT experts who say something is not safe but don't understand what can be made safer. This is a limitation on functionality and that is why it is important to have someone who can hold the conversation with both the IT and business sides. Housing associations need guidance to ensure these functions are well-protected in their own organizations. It is killing when

the knowledge remains with external advisers. It is often too complex and comprehensive to put everything on one person. When we were smaller, I also had the idea that I could encompass everything, but in the meantime, I also have a team around me because I also don't know everything. That is why it is important to have a team with multiple expertise and from multiple perspectives.

Cyber threats and your organisation

6. If you have not yet experienced a victim, is there a real threat of a cyber attack in the housing association sector in your opinion? Why?

   It's important to be aware of the attacks on IT systems, as they are becoming increasingly common, especially from Russia and Africa. In some cases, they are even companies that professionally hack organizations. It's no longer just a underworld happening, it's become a profitable business. When I gave presentations a few years ago, I often used examples to show this, but since the University of Maastricht was hacked, awareness among non-profit organizations and executives has risen. It feels like there are people continually trying to break in at your door, just like if you had a camera that shows you people coming to your house to check if the door is open. It's a permanent problem and it's becoming more and more palpable, as far as that can be.

Cybersecurity

7. Do the housing associations you have worked with use cybersecurity frameworks (such as NIST, ISO 27001, ISO 27002)? If so, which ones and why? Do you think housing associations should work with these frameworks?

   We have been working with ISO 27001 for a long time, because it's a complete framework that helps us secure our software. We have been certified since 2007 or 2008, when the ISO began. The nice thing about this framework is that it provides a clear structure, which gives the feeling of completeness. I also see that it constantly renews itself, but still works with the same concepts in the IT industry. Although many concepts remain the same, we now have to look at a larger context, because technology is developing. I wonder how many housing associations have an ISO certification.

8. Do the housing associations you have worked with often have a cybersecurity specialist on staff? Why? If not, should they have a cybersecurity specialist on staff?

   "I rarely come across specialists. There are IT professionals who have an interest and above-average knowledge, but I don't often come across true specialists.

   Q: Is it a good idea for housing associations to consider hiring someone like that?

   I think it can be difficult to keep someone truly passionate in their work. Because how exciting is it if you often have to have a general profile because the organization and the amount of work is not that large or

complex or varied, and therefore not in need of many specific specialists. It's always better to work with specialists in different fields, but it's important to have someone who understands and is able to lead. That's more important than someone who knows it all themselves. For example, our housing allocation system. We've hired an external party to do a pen-test, but there are very few people who actually understand what such a test entails and how it needs to be repeated regularly and how you can test more specifically and effectively. By hiring an external expert, you're buying a sense of security, but the internal understanding is often minimal. It would be better if housing association board members would get more of a feel for what they're having researched and what the value of that is, and if they would seek more support in that area. I think they've been doing that more in recent years, but I'm not really impressed by the quality of it.

9. How does your organization currently stay informed about current cyber threats? How could your organization stay even better informed about current cyber threats? How could housing associations stay informed about current cyber threats?

   We are a group of people who are professionally involved in IT. We have an architect in our Information Security Management group who keeps himself permanently informed of developments in the industry through participation in congresses and conferences and by reading a lot. We also have a management cycle in which we train our employees and we work together with experts from our hosting partner, Finity, who have a large security team. We also deal with technical developments of major players such as Microsoft. I am also responsible for the legal side of our activities.

   Q: And do you see the same being tried at housing associations to also stay informed of current threats?

   Yes, that is more. But to some extent it is also correct. Our customers of course expect us as suppliers to play a role in this. And they also find that in many cases we should take our responsibility. But when we try to explain this or make extra investments, it often becomes a legal or financial story. I find that unfortunate, because it is actually as if you expect your landlord to put a deadbolt on the door and install an alarm when there are more and more burglaries. That's not logical. But with us, it is often expected that we will take care of this, while the housing association also has a responsibility in these matters. The conversation about this can sometimes be difficult, especially because it often concerns money. Yes, and liability also plays a role.

10. Do you see many housing associations working together or seeking partnerships in the area of cybersecurity?

    Yes, our experience has been that it's hugely stimulating to discuss privacy and security in our user groups. Unfortunately, we find that people from the business side often find it difficult to engage with these complex subjects. But, for example, when a fraud investigation takes place, or there's an attempted hack, attention is refocused on these topics. As the major incident in Brabant this year has shown, everyone becomes alert

again to these issues. That's why we try to encourage our user groups to collaborate structurally on privacy and security. However, it's difficult to get people to be proactive in this area, they're often reactive. It would be nice if we could continue to have conversations about responsibility in this area, because it affects all parties. Some phishing incidents come from a weak link at the user organization, rather than at the IT supplier. When we have these kinds of conversations, we wonder how housing associations deal with this and whether they keep us informed if an incident takes place, because that may also affect us. However, it's difficult to determine who is responsible and how the roles are divided. Moreover, as a supplier we are also dependent on payments from our customers, which can sometimes lead to difficult situations. It's always a search for balance.

11. Are the housing associations you have been at sufficiently secure against a cyber attack? Why or why not? What still needs to happen?

    Unfortunately, I cannot speak in general terms. For our applications, we do our utmost to make them as stable as possible. Fortunately, we have had very few incidents. Although I do see incidents occasionally at other housing associations, I wonder how it is that this doesn't occur at our company.

IT risk management and your organization

12. Is there a formalized (IT) risk management policy at the housing associations you have been at? And when does this date from?

    In the projects we work on, we come across it very little. We often mention it in the first instance and can only assess it based on the scope of the project and the use of the product. But I notice that DPIA's are often viewed from a privacy perspective and that there are very few organizations that carry out a DPIA themselves, even though it is the responsibility of the data controller. All to make a risk assessment, what data do we have? What measures do we have for this? It's also something that you don't do once, but it should be done regularly. I can also understand why it doesn't happen often, because although we do it, it's also difficult to do. It's a journey of years to develop a good risk inventory method and link it to measures and to measure it. Our Dutch mentality is perhaps focused on opportunities and we think less in terms of risks. The idea of zero trust is mega complex. The zero trust mentality in combination with risk management does not fit well within our culture and working methods and it will take another 10 years to find a good balance between security and workability.

Risk identification, Risk analysis, Risk Evaluation (Risk assessment)

13. How are IT risks identified in the housing associations you have been at?

    In general, I think risk scans are mostly carried out by consultants.

14. Who should determine the risk appetite in a housing association?

    Yes, that is also broad. It is a mix of technology, legal and business. That's why you need someone who leads that and combines all those different disciplines. When it happens, it usually happens from an IT perspective.

15. Are risks in housing associations classified in a standardized way (chance * impact)? If not, should this be done?

    I believe that it can be very helpful if you have smart tools that can classify risks and indicate measures to manage these risks. For example, we use ISMS online, an English tool for the ISO that has a risk matrix with chance and impact, where you can indicate frequency and policy measures. By assessing the effectiveness of the measures and repeating this process regularly, the plan-do-check-act cycle comes back well. I think this can sometimes be complex, especially if it's not in your DNA. But I think this kind of tooling is also often seen at housing associations. Personally, I do not think ISMS online is ideal and I hope that in the future more tooling will come from NEN. Sometimes we have even considered creating our own tool to manage repairability through operational management tools.

Monitoring and reviewing

16. Are the risks at housing associations evaluated and reviewed on a periodic basis? What should be periodic?

    Whether it's the risk management methodology that you as an organization want to adopt, I don't believe in going through a checklist once a year. It needs to come back more often. I don't know if you've ever done it yourself, but for example, if you describe a risk and name it, making the translation into what that practically means for you and what you're doing to mitigate that risk is very complex. So you also need to be able to think at an abstract level and sometimes you need to think back to the reason why you're doing something. For example, if we do this, we're not running that risk. So it also depends on the operating procedures. People who do something will never look in the manual, because they know what they're doing. But sometimes you do need to look at whether what we're doing is still logical. This takes time and money and you need people who enjoy thinking about this. Advisors also have a role, but they also need to be creative to stay out of those lists and make it concrete and practical. It's best to do it frequently, so better small steps with a high frequency than long complex lists where you think you've had it for the next year. Because then it just doesn't work.

17. Are the risk assessment methods evaluated periodically at housing associations? If not, should this be done? And how could this be done best?

    I would like to see it come back in user groups. Could it come back on a regular basis? So both sharing information and discussing. We have taken measures to limit the risks, but are these still effective? It would be nice if we could consult with a mix of people, such as technical and legal experts, on a regular basis. For example, every six weeks. I have worked with a housing association before, but they felt they had to do it themselves. The new IT manager said they had to start it themselves, so it doesn't have to be with external help. I am interested and don't count the hours. But I don't know if it still happens, because it's been a year, but it hasn't been done since. I understand that it is difficult to make time in your daily work with tenants and housing, but IT systems are becoming increasingly important and it can go wrong once.

18. How can the periodic execution of the IT risk analysis be best ensured?

    Ultimately, there is always someone responsible, but in this case, I think the person who carried out this action was not. The funny thing is that the hired lawyer I spoke to was also detached as a security officer, and that was already an issue. But why didn't they choose a permanent employee who has the right skills and enjoys doing this long-term. Instead, they choose to hire an external person with the risk that he understands how it works. But at some point, that person leaves again. Furthermore, security suddenly becomes very expensive when you pay €150 per hour.

    Communication and consultation

19. In what form should the risks be best reported to management?

    It's a dilemma, I can see it myself. The dilemma around reporting on the risk methodology within the executive team. We have a commercial and technical director, and they're happy for me to handle it. It's difficult to make the report understandable for a wider audience without making it too complex. The challenge is to make the translation of what the impact is for people's daily work and to make it understandable for them. It's important to remember that people prefer to be unconsciously competent and that they naturally work safely and well without always understanding why they do it. So, someone needs to think about it and make it understandable for a wider audience.

20. Do housing associations often have an action plan / roadmap for mitigating identified risks? How could this look best?

    I don't get much input on this. I would welcome it if it was available and on the table, and there could be a conversation about it.

21. In your opinion, are the IT risks within housing associations sufficiently covered? Why or why not? What still needs to happen?

    There seems to be an intensification in the standardization within housing corporations, and there is also an increasing awareness of this. For example, a Vera, where data standardization takes place, Aedes is also involved in this. The challenge is to make the connection to the daily work of the employees and to reduce the complexity of this. Some employees simply carry out what they have to do without really knowing why this is so, so it is important to give them good and safe instructions and explain why things are done in a certain way. We don't see everything within housing corporations. It's difficult to have a substantive conversation with each other regularly, especially since we often talk to people who focus on the business, the user side or IT, or lawyers. It would be nice if this initiative came from the housing corporations to have this conversation, but this doesn't happen very often.

    Privacy & information security within your organization

22. How can housing associations ensure that information is always available (availability)? Is this already being done well? Is it often done via outsourcing?

Yes, I think so. We have always worked in a web-based way. That means that if nothing is running within a housing corporation, it is our responsibility to make sure that our service can continue. We have a lot of experience in this. It's nice that, even if everything within a housing corporation stalls and no longer works, they can still continue with our applications. Our applications are also loosely coupled to other systems, which means that they are partially dependent on input, but can also function independently. This is not true for all applications, but it is for many of them. The housing allocation application, for example, is one of the largest and can function completely autonomously, even if there are no automatic payments coming in. But it's also possible to update this manually. For example, if it says on paper that a housing has become available, you can update the housing stock in the system and the distribution can be done fine. So, our housing allocation application can function perfectly in a standalone way.

23. How can the integrity of information within housing associations be properly ensured? In other words, how is the information protected against unauthorized or unusual modification or destruction? Is this already being done well?

    Yes, there are the availability, integrity, and confidentiality. Those are three different aspects. When we look at integrity, it has a lot to do with the quality of the software code. So, whether what you see is correct and whether the right people are in the right places and whether the data is reliable and the processing is reliable. We pay a lot of attention to that, so we focus on secure coding, good checks, and good logging. That is complex and sometimes it goes wrong, but we test and maintain it permanently. Because that's our job. A large part of our work is about integrity and another large part is about availability, which is the infrastructure under the web application. As for confidentiality, it becomes more complex, because the user and the corporation itself also play a larger role there. So do they have good authorizations set up and do they make use of the security options and do they have good key management? We often do not know how well they have arranged that on their side. We have experienced fraud situations in the past where someone does something through someone else's account that should not be there. We can trace that back through logging, but our systems are not yet fully built on a zero trust model, we also need input from the associations, what is their need and what do they want in the future? We have been saying for a long time that we need to move towards a safer access, but that was difficult, because for housing seekers it was already complex enough. So we first had the discussion about how secure a password should be, because they could not remember it. I understand what you mean by security and user-friendliness. So we need to find a balance between security and user-friendliness, this also applies to housing associations.

24. How do housing associations comply with laws and regulations regarding privacy? For example, through compliance with the GDPR? Is this already being done well?

You can see that the influence of advisers results in getting more questions. In the past, we had more information the better and kept more historical data, where we collected more information, it was important to keep everything. Over time, we have built in certain mechanisms to clean up the data, but many corporations still like to keep all historical data.

25. Are all actions within housing associations checked in the various information systems? (Auditability) and how is this done? Or how could this be done?

    They don't have much monitoring. Only in case of incidents. But when they happen, we want to keep track of them, because it's a part of "zero trust mentality". Which means we think from a risk perspective, and assume that no one can be trusted. Nobody wants that, but sometimes it's necessary to take specific actions to prevent something from happening among colleagues. For example, I asked our accountant if we can see who logs in to our administrative system outside of office hours through log files. This is because the administration works during the day, and I sometimes work at night too, but it's interesting to know what's happening outside of office hours. A housing corporation could also ask who is not logged out or what actions were taken outside of office hours, for example, in the case of housing allocation. It's easy to implement, but for this a certain "zero trust mentality" is required, or assessing a risk that we don't entirely trust what someone does outside of collegial supervision.

26. Are the information systems at housing associations regularly cleaned up? Irrelevant information removed?

    I notice that it happens sporadically, so it happens less often than I would like. I think, specifically in the area of data minimization, that you can still adjust your application in a more specific way. There is still room for improvement there.

27. In your opinion, are improvements needed in all of the above aspects? If so, which ones? Why?

    I approach it from the zero trust principle, both in terms of how it works and what employees need to be able to do. That's very different from just thinking about what's easiest for employees. Maybe we should also think from a different angle and facilitate looking at things from the perspective of business risks. It's also difficult for us to think that way, but it's necessary. From an architectural perspective, it's good to look for compromises and sometimes measure things to see what works. We also see in the banking industry that AI is used to detect suspicious patterns in the many movements and transactions that take place. We need to be careful with this information, but I think we can use it to feed zero trust. There's also something to be learned from this.

28. Is privacy and information security adequately safeguarded within the housing association sector? Why or why not?

    I think it's important to mention how I see the situation. I didn't think it was that great a couple of years ago, but it has improved. Still, I would

only give it a weak 6, because the complexity is underestimated and there's a lot of talk about liability, while willingness to invest in security is limited.

Q: I wonder if this is due to a lack of awareness or if it's a matter of priorities?

It's seeing the need but not being able to translate it into the impact. It's like with houses - new houses are safer than older houses, because they were built with today's technology. This also applies to many IT facilities, something that has always functioned but sometimes needs new technologies to be added. This costs money and we're willing to make those investments, but it's not only our responsibility. So the discussion is whether we want to move towards a collective three-star lock or if we think the current lock is good enough, because it also shouldn't be too expensive. Some people have an alarm system at home and others have three-point locks, but some security measures are more common now than before. If we work better together, we can make big steps and the costs won't be so high. I notice, however, that the willingness to invest is limited and people quickly say that it's our responsibility and that they pay us for it. But in the end, we have to ask what it's worth and what the customer wants. If we do this together, we can add more value and it's not just a matter of making money. It's also about creating a sustainable relationship and working together to improve security."