Research on why Dutch Public Organizations fail to grow to sufficient maturity levels in information security

UNIVERSITY OF TWENTE.

Master Thesis – Business Administration

Topic of research
Information Security within Dutch Public Organizations

Supervisor
Dr. J.H. Bullee
Second supervisor
Ir. B. Kijl
Company supervisor
-

Author:
Marcus Coskun
S2506513

20th of March 2022

Abstract

Introduction: Headlines in newspapers about data breaches, security incidents or even hacks at Dutch Public Organizations are increasing. Therefore it could be of interest to conduct research focused on information security practices at Dutch Public Organizations.

Objective: The goal of this research is to gather knowledge about the factors that play a role within Dutch Public Organizations, that disables these organizations to make further progress and grow in maturity within information security practices to prevent data breaches and hackings. The research question within this research is: *"Why are Dutch Public Organizations failing to get their information security on sufficient maturity levels and what could they do in their approach to information security practices to increase these levels?"*

Method: A qualitative study with semi-structured interviews was conducted with different people from different types of organizations. The first group of respondents consisted of 3 IT-auditors and/or IT-advisors working at a respected accounting firm. The second group of respondents consisted of 7 people considered experts on information security matters since all of them work at Dutch municipalities in the role of Chief Information Security Officer or Team Manager Information. Through thematic content analysis all interviews were analysed after transcription and the most frequent mentioned factors in struggling with information security maturity levels have been identified.

Result: It was found that there is no one unanimous reason for why Dutch Public Organizations are not growing in maturity. There are multiple factors present which play a role in hindering Dutch Public Organizations in growing in information security maturity levels. These factors and elements variate and differ from an external IT auditor viewpoint compared to internal viewpoints of the participating respondents such as CISO's.

Conclusion: Since this research is focused on factors and reasons that hinder growth in maturity from two perspectives, it can be concluded that these views do not deviate much. Therefore it also can be concluded that the most important elements that hinder growth are capacities based on different grounds, such as expertise, staff and a lack of time. Additionally, there is lack of fulfilment of PDCA cycles which ensures there is no sufficient evaluation or monitoring in measures taken. Furthermore, it can be concluded that a lot of processes are not yet defined which translates in lack of knowledge about roles and responsibilities.

Keywords: Information Security, Maturity, Dutch Public Organizations

Preface

Hereby I would like to present my thesis about information security within Dutch Public Organizations. This thesis is the last and final part of completing the Master of Science in Business Administration at the University of Twente. The motive and purpose of this research were proposed by Company X.

Overall, I would like to take this opportunity to thank everybody that participated within the IT Advisory department at Company X and especially the ones who helped during this research: Person 1, Person 2 and Person 3. Special thanks to my supervisor Person 4 who helped me with input, guidance and most of all motivation to keep on going.

In addition, I want to thank my thesis supervisor Jan Willem Bullee for his guidance, time, weekly interesting sessions and his feedback during the process. Next to that, I want to thank my second supervisor Bjorn Kijl for taking time and effort to read my thesis and provide me with important and helpful feedback.

Last but not least, I want to show and express my gratitude to my family, especially to my parents who always believed in me, whatever choice I made. But most of all, I would like to thank my wife Minerwa for her understanding attitude, patience and love, the whole period during my study and this research.

Marcus Coskun,
March, 2022

Table of content

1. Introduction **5**

1.1 Problem indication *5*

1.2 Research goal and relevance *7*

1.3 Structure of study *10*

2. Literature review **12**

2.1 Information security *12*

2.2 IT Governance *16*

2.3 Tools for growth and maturity measurement *18*

3. Methodology **27**

3.1 Research design *27*

3.2 Research model *27*

3.3 Scope and sample *27*

3.4 Type of research *28*

3.5 Research method and data collection *29*

3.7 Analysis *31*

3.8 Exploratory interviews *32*

3.9 In-depth interviews *33*

4. Results **34**

4.1 Analysis of exploratory interviews *34*

4.2 Analysis of in-depth interviews *41*

5. Conclusion and discussion **55**

5.1 Key findings *55*

5.2 Recommendations *57*

5.3 Limitations and future research *63*

References **65**

Appendix I: Maturity models **70**

Appendix II: Interview questionnaire I **71**

Appendix III: Interview questionnaire II **72**

Appendix IV: Information Security Governance Framework **74**

1. Introduction

This first chapter introduces the topic of this study and suggests the relevance of this research. Furthermore, this chapter defines the problem indication, research setting, research question, and the structure of this research.

1.1 Problem indication

Protecting information is of high importance in current daily business topics, this ranges from the highest layers within governmental institutions and public organizations to information concerning data in forms of personal data and trade secrets (Dzazali, 2009). For this reason, information security becomes more important every day and is therefore considered a crucial asset for organizations. Role and importance of protection of data increases in large organizations, while small and medium enterprises (SME's) struggle with this case since development and adoption requires effort in multiple ways and several factors like time and resources (Kaur, 2013). As technological systems are increasing in size and grow more sophisticated, threat of security is growing as well. An example of quite a recent incident is the case of the municipality of Hof van Twente in the Netherlands. A case which became public in December 2020, but already started a month earlier, on the 9th of November 2020. A system engineer changed the password for a controlling account to 'Welkom2020' in October. And after changing the security firewall in November as well, hackers found their access into the servers already on November 9th, 2020. This case illustrated that the combination of human error and lack of control frameworks, can lead to major incidents. Incidents like the hacking of an ICT environment of governmental institutions, in the form of a municipality. This gave hackers access to privacy sensitive information of citizens. Besides, it made them able to shut down servers, resulting in employees that could not access systems and data, not being able to carry out their daily tasks. An independent cyber security firm later concluded, that the system engineer was mostly responsible for this incident. However, the municipality itself is not without any blame. They were accused of lack of alertness and trusting too much on the expertise of one person, without sufficiently assessing security policies by external parties (NOS, 2021). This example shows that certain incidents can badly harm integrity of governmental institutions. Moreover, it also shows the importance of setting requirements in the field of security of IT systems, such as password management.

Furthermore, more importantly, the example about Hof van Twente, illustrates the importance of the human factor and the role humans have and should have in the field of information security. Schneier (2015) concluded that the user is usually the weakest tie in the security chain. In addition, the factor of mandatoriness makes employees act in accordance of information security policies (Boss, 2009). In spite of mandatory rules, many of needed processes designed to protect information are still to a large extent dependent on human behaviour, by cause of negligence or lack of knowledge (Van Niekerk, 2010). Additionally, issues regarding information security are best challenged through adaption of certain skills needed for change of organizational culture and effective communication between Chief Information Security Officer (CISO), Information Security Officer (ISO), end users of applications and systems and other layers in management and organizations (Ashenden, 2008). Within the context of digital transformation and risks that result from Industry 4.0, challenges around security are rising, devices and data grow exponentially while lack of standards and adoption of security still exist. Additionally, Malecki (2020) states that the recent Covid-19 pandemic causes a risk since millions of employees of organizations are working remotely and in digital environments from their home offices, far away from the organizations offices, making the protection of information and data more important than ever. For this reason, security of data and information must be developed to higher levels (Bligh-Wall, 2017). Therefore it is of importance to examine what factors play a role in the process of the lack of growth and improvement in information security practices. Additionally, rules, regulations and policies regarding information security are not set and developed sufficiently enough everywhere around the world. Many are still without sufficient regulations or guidelines set by governments, in protection of data and information. Besides, not all countries are aiming for the same purposes, there are countries that refer to security goals, whereas there are countries that aim at specification of detailed implementations (Johnson, 2014). This implies that countries differ in approach. Countries which refer to security goals, are further developed in their protection of information and data and therefore further developed in terms of stages of maturity in information security. In the field of assessment of organizational performance and improvement of performance, maturity models can be used for this case. With the help of maturity models, analysis of strengths and weaknesses becomes more easily visible. Maturity models can help in assessing this and additionally conclude what actions are needed for growth (Khoshgoftar, 2009). Other research states that IT auditors involved in information security topics, experience that organizations struggle with implementing the correct measurements and tools for protecting their IT systems and data. Leading to security incidents with all data loss, damages and other risks as a result (De Lange, 2015). The Information Security Service for municipalities (Informatiebeveiligingsdienst: IBD), an initiative of all Dutch municipalities, provides an overview of numbers and notable incidents around information security of the past year. In 2020, the IBD received 3845 questions and notifications around information security, next to registration of 175 incidents where help, coordination or support was needed for municipalities (IBD, 2021). While in 2019, the IBD received 3044 questions and notifications about privacy and information security matters. Additionally, the Computer Emergency Response Team (CERT) of the IBD sent out 1751 vulnerability notifications including 23 'very serious' cases with a high chance of abuse (IBD, 2020). Whereas in 2018, the IBD received 1373 questions and notifications, while 179 incidents were registered and the CERT sent out 2049 vulnerability warnings. This is a yearly increase of around 26% from 2019 to 2020 and 121% from 2018 to 2019 in only questions and notifications.

Overall, the above demonstrates the importance of information security and the need for organizations to consider serious actions towards information security practices. And at the same time, become more mature with the help of assessment through maturity models.

1.2 Research goal and relevance

Most recently, in November 2021, hackers have gathered access to the account of an employee of the municipality of Ede, the Netherlands, and have been able to send out a large amount of phishing emails to other emails (De Gelderlander, 2021). Experts raise different questions with regards to this new situation. Firstly, the municipality of Ede was victim of a hack in 2016 as well. Therefore, experts wonder how it is possible that after the incident in 2016, this new incident happened. After examination of the first incident, the organization concluded that security regulations were not structured and documented thoroughly. Therefore, the organization acted upon and took new measures regarding security. Additionally, they raise the question about the possibility that after such new attack, nothing happens when the account of one person, sends out thousands of emails in a few hours. This food for thought feeds speculations about if higher information security practices and higher maturity could have prevented situations like these. Another incident, which could have ended much worse, was the hack of the municipality of Lochem in in June 2019. Hackers found their way into the information- and communication technology system of the organization, but the attack fortunately was noticed before things became even worse. However, this attack caused that the organization was not able to be remote and active for more than a day. The municipality of Lochem announced that this attack caused damage for around €200.000. The same municipality was victim of likewise attack in 2015 as well. A virus was spread out over the systems of the organization, which encrypted files, resulting in employees that could not reach their files and programs (De Stentor, 2019). Since there are municipalities that suffered more attacks over the last years and other municipalities that were damaged by attacks so hard, it can be stated that these recent examples argue that maturity in information security of these municipalities was not of a sufficient level.

These recent situations, show that information security within Dutch Public Organizations is an important topic and needs high priority. This research attempts to examine what hinders Dutch Public Organizations in their approach to information security practices and why they fail to reach certain maturity levels. Next to that, research will be done to find out which factors and methods can have an impact on increasing the level of maturity, based on the available maturity models literature, within Dutch Public Organizations on grounds of information security. Therefore, the central research question formulated in this study is: *"Why are Dutch Public Organizations failing to get their information security on sufficient maturity levels and what could they do in their approach to information security practices to increase these levels?"* To be able to answer the central research question, sub-questions are needed in order to maintain an adequate result for research. The following sub-questions which are needed, are formulated and listed below with a description;

First of all, it is of importance to explore the term of information security, to understand the context of which research is about. Moreover, it is needed to discover what the term of information security covers:

- What is information security in a general context?

Secondly, since the aim of this research is to research why Dutch Public Organizations are failing to get information security on sufficient levels, it is important to look into models and frameworks that cover the field of information security combined with growth:

- What models or frameworks are available in existing literature that could help organizations grow to higher levels in information security?

Thirdly, to understand the need of growth and to achieve higher levels of maturity, it is important to gather knowledge about the current situation of Dutch Public Organizations. It is needed to assess what levels Dutch Public Organizations are now, in order to understand the emergence of the current situations:

- What is going well with Dutch Public Organizations and what do they need to improve in their current maturity levels?

Fourthly, the value of the existing frameworks in maturity for Dutch Public Organizations is yet unknown. For this reason, it can be of value to further explore what existing models add and if they are even being used in development of policies within organizations to further develop information security practices:

- What is the added value of existing maturity models (NBA) in achieving sufficient levels in information security?

Fifthly, in order to know what accountancy and consultancy firms can improve in their contribution of development in information security practices within Dutch Public Organizations, it is needed to collect information around this subject, from Dutch Public Organizations themselves. It is through this way, that the gathered information can turn into recommendations from Dutch Public Organizations to accountancy and consultancy firms in what they can deliver and contribute:

- What can accountancy and consultancy firms do, in order to help Dutch Public Organizations grow in their transition of increasement in maturity levels?

While risks of low level maturity of information security are commonly known, accountancy and audit firms experience lack of sincere interest in this topic and intentionally achieving higher levels of maturity. Therefore, this research could be beneficial to discover why Dutch Public Organizations fail to achieve higher maturity levels and what could drive and trigger Dutch Public Organizations in achieving higher maturity in information security. The goal is to find out what discourages and more important, what can encourage Dutch Public Organizations to achieve a higher level of maturity. Additionally, by researching the variables and factors that can increase maturity levels of information security, this could possibly result in answers for (consulting) firms to gather knowledge on how to adapt and to know what strings to pull in effectively serving public organizations.

Previous studies have demonstrated that besides concretization of frameworks, multiple other variables can contribute to successful implementation of cyber security for smaller (e)governmental institutions (Somers, 2021). Moreover, Schneier (2015) proposed that future research on information security chains should not be solely pointed towards technology, but more to people (users), goals and processes. In addition, Khando et al. (2021) conducted a systematic literature review on factors and methods enhancing awareness on information security on public and private organizations and concluded that methods such as gamification and guidelines, factors like management support, culture, education, training and several other factors have an impact on increasing information security awareness among public organizations.

Whereas studies about factors that hinder growth in information security within Dutch Public Organizations and why they fail to reach certain intended levels and variables, that can increase maturity of Dutch Public Organizations are not yet conducted. Therefore, it could be of interest to conduct research on Dutch Public Organizations. More specifically on municipalities in the public sector.

1.3 Structure of study

The structure of this study is divided into different chapters. To begin with, the first chapter provides an introduction of the topic, problem indication, research question and relevance on base of theoretical and managerial manners. The second chapter gives an overview of the literature and existing knowledge about information security, governance and IT governance among other related subjects. In addition, the third chapter explains the methodology used during this research of study. Furthermore, the fourth chapter gives an overview and analysis of the results gathered during this research. Therefore, the fifth and last chapter consists of conclusion, discussion, further research possibilities and business recommendations.

2. Literature review

The second chapter introduces the main topics of focus of this study. Existing relevant literature and knowledge about information security, IT governance, information security within public organizations and maturity models will be further explained. This part is a result of desk research in existing literature. In search of subjects that need further explanation and clarification, in order to understand the important factors that play a role in the achievement of higher maturity in information security, or the possible understanding of lack of achievement in this subject. The subjects are selected for research because of their relation to the field of information security within Dutch Public Organizations. First of all, general analysis of literature about information security is provided because it is needed for understanding the context of information security and the field it covers. Secondly, since the topic is related to Dutch Public Organizations, it is important to understand about what matters play a role in governance in this field. Lastly, it is of importance to provide a general understanding about models available to use within business topics, but more specifically models available for Dutch Public Organizations that can be used to achieve growth in the field.

2.1 Information security

Security in general, is associated with the protection of something, while speaking in organizational terms, something is most often associated with assets of organizations. Whitman and Mattord (2009) describe information security as *"the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information"* (p. 8) (Whitman, 2009). Furthermore, Whitman and Mattord (2009) define characteristics regarding information security, making it valuable characteristics in organizations. Characteristics as confidentiality, integrity and availability as these are also mentioned in ISO/IEC 27002. Confidentiality can refer to an organizations attempt to having data secret, meaning that people who have access must be authorized. Integrity refers to correctness and quality of data while availability refers to information as a resource that is available when needed. These three characteristics are also labelled as the CIA triangle. However, Whitman & Mattord (2009) argue that this 'CIA triangle' cannot solely cover the present environment of the computer industry which is constantly changing. Therefore, Whitman and Mattord (2009) reckon accuracy, authenticity, utility and possession as characteristics that are in need of protection. Accuracy refers to the preciseness of the information that is kept in store, while authenticity can refer to the trustworthiness and origin of the data, whereas utility refers to the usefulness of data and possession involves around ownership of data. Security and protection of information in digitalized manners already became an important topic in organizations in recent years, and is increasing in importance still.

Since technological transformations, the storage, processing and transferring of data has increased revolutionary. Overall, IT can be responsible for this whole process of storing, transferring and processing of information. These elements combined with use of internet and other IT related systems, vulnerability variables appeared as well (Moormann, 2006). Before the common usage of internet and IT, transfer and process of information was slow, manual and analogical. Moreover, the processing of storage of data and information was literally fulfilled in warehouses. Looking back, this period was characteristic for how easy information could have been stolen with all further risks coming along. Moreover, information security during this period must be seen in context and perspective, only few people had access to the storage of data and guards protected warehouses to prevent unauthorized access. The revolutionary increasement of usage of internet, processing of information and data has also been through extraordinarily increasement (Moormann, 2006). As with other positive development, among this increasing usage and development of IT systems and information processes, other wrong intentions arise as well. Criminals and hackers can enter organizational systems and subsequently unnoticed steal and capture data. The increase in data processing enabled through development of technologies comes with negative effects as well, with risk of data theft and breaches for example. Therefore, traditional information security has developed into serious discussions and matters within organizations. Since organizations need to develop capabilities which can be complicated, in order to be resistant to diverse forms of attacks on information and data to ensure confidentiality and integrity within the organizations usage of information (Moormann, 2006). Since the risks and consequences that come along with cybercrime have seen significant increasement and organizations in both the private and public sector are still behind when it comes to sufficient adaption to measurements regarding information security. Hence, governmental laws and regulations are set up in order to move organizations to consider information security as an organizational priority. The need for managed systems in order to optimize the protection of information and data is documented in guidelines and certifications such as the ISO 27001. The implementation and improvement of implementation, maintenance and the continually improvement of information security management systems is documented in ISO/IEC 27001:2013 (ISO/IEC). Moreover, it can be seen that there are several theories and literature available in the context of information security, also the importance is known. However there are also models that dive deeper into information security within organizations and organizational context, which need further clarification and explanation.

Business Model for Information Security (BMIS)

The Business Model for Information Security (BMIS) which can be seen below in Figure 1, offers an approach to information security that views the organization as *"an organized collection of parts that are highly integrated to accomplish an overall goal"* (p. 10) (von Roessing, 2010). The approach that is defined from the perspective of Von Roessing (2010) offers a framework which is put in a broader perspective related to the organization. Mainly compared to other more traditional approaches, which are more reactive and particularly considered from an IT perspective. The four elements in the model illustrate the main areas in where and how information security is incorporated.

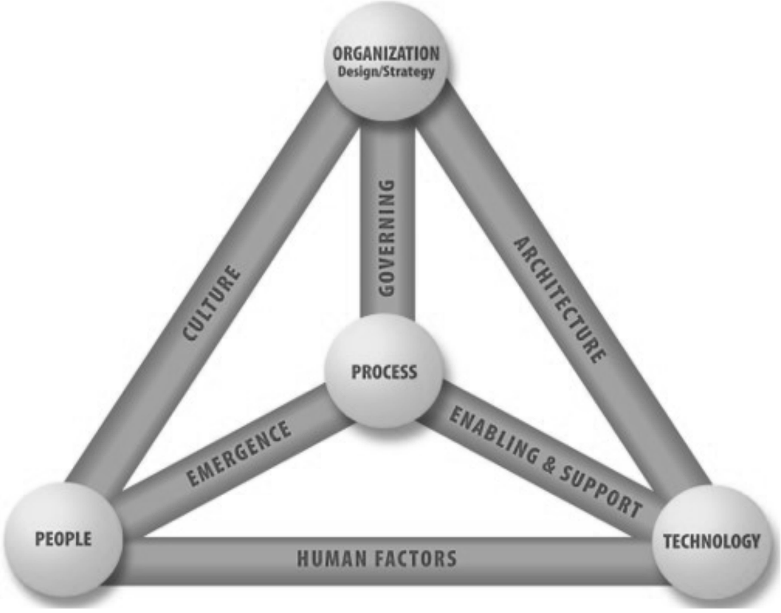


Figure 1: Business Model for Information Security

Moreover, the BMIS offers a ‘systems thinking approach’ which is mainly achieved by the four main elements from which the model consists. These four elements represent different perspectives of the organization, as a whole and the connections between the different elements. The four elements within the model have a dynamic connection. The four elements and their explanation and focus are explained by Kiely & Benzel (2006) as:

- *Organization*: this element focuses mainly on the need of organizational structures and strategies, which can enable the organization to effectively compete in order to design competitive advantage. Moreover, it gives an understanding of tolerance to risk and adaptation of governance which labels security as a priority. This element attempts to urge the organization to include information security capabilities into strategies. An example that could belong to this element can be appointing certain people or departments with roles and responsibilities regarding information security.
- *Process*: this element aims on providing a perspective on information security that are based on formal and informal mechanisms with a focus on how processes and business goals are realised within the organization. An example that could belong to this element can be the formalization of periodical audits in assessing efficiency in information security.
- *Technology*: the element of technology explains itself as the development and implementation of technological approaches and needs in order to protect information systems. Moreover, the approach of technology should stay ahead of technology to which the organizations technology is being threat. An example in the context of information security could be the implementation of IT controls.
- *People*: the element of people mainly focuses on resources in human forms within the organization, further than fundamental security but in additional training as well. An example in this context could be the appointment of cross-functional project teams that have a strong focus on goals towards information security practices.

The four elements of the model are connected through six lines because these define the dynamics of the elements between each other. These connections are described as: governing, culture, architecture, enabling and support, human factors and emergence. Additionally, important to mention is that the connections between the elements also demonstrate the conflicting role between them at the same time (Kiely, 2006). Roessing (2010) explains governing as the interconnection between theory and practice around corporate governance. Culture is described as a wide interconnection within the model because it entails factors around human behaviour, habits and actions. Moreover, the interconnection focuses on the overall culture and perspective on information security within an organization. The interconnection of architecture outlines the relation between the organization and technology since there is a need of strategy and design to be implemented when there is need of implementation of technology in business. The line of enabling and support points out necessity between technology and the organizational process. The main focus of this interconnection is pointed at integration of control frameworks, standards and compliance. The human factor link identifies the existence of usage of technology by humans and their behaviour which according to the model is subject to change in technology through challenges coming along technology usage. The sixth interconnection of emergence addresses unpredictability and the presence of the emergence of patterns into the model. The interconnection describes that defined processes around core businesses of organizations will change inevitably.

2.2 IT Governance

IT governance emerged as a prominent issue within the information technology field in organizations in recent years. Additionally it became an important issue of discussion in most organizations by attempts of implementing fusions between different departments of organizations to obtain involvement from higher levels of management (De Haes, 2004). Research states that there is no one way definition of IT governance, De Haes and van Grembergen (2004) for example, define IT governance as *“the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategy and objectives.”* and state another definition in the same research context as *“IT governance is the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT”*. Differences in earlier definitions are present, meanwhile it is notable that both have a focus on same aspects since both want to achieve a link between business and IT (De Haes, 2004). Since information security can be considered as a topic that is notable to IT related topics and tasks, IT governance needs to be analyzed within this research of growth in information security. However, analysis of IT governance is possible via multiple manners. Weill and Ross (2004) for example, consider IT governance as arrangement of decision making and structure of accountability to encourage the desired behaviours in the usage of IT while other possible manners of analysis consider IT governance as a perspective from which IT decisions take place (Weill, 2004). Overall, other research by Weill and Ross (2005) concluded that there is no formula or anything like, that can suggest easy implementation of IT governance measures. However, well thought-out governance designs must be able to benefit organizations in achieving strategic objectives (Weill, 2005).

However, since this research has the focus on the information security practices within Dutch Public Organizations, is important which IT governance mechanisms and standardized frameworks are being considered in the Netherlands that need to be applied to these organizations.

Information security within Dutch Public Organizations

In order of protection of organizations and their clients from cyber criminals and other forms of misuse, governmental institutions have created laws and regulations that define requirements in how organizations need to handle and protect data. These regulations can differ around the world, while they serve the same purpose, to strengthen compliance in protection of information. Since the beginning of 2020, Baseline Information Security Government (Baseline Informatiebeveiliging Overheid: BIO) has been formed and resulted into the combination of the information security standards for central government, municipalities and other Dutch Public (governmental) Organizations (Digitale Overheid, 2021). In fact, the BIO can be seen as a supplement of the ISO/IEC 27001:2017 and ISO/IEC 27002:2017 for governments. Meaning it is not replacing the rules set by the mentioned ISO/IEC but is an adjustment designed for Dutch Public Organizations to implement at least. The BIO is assumed to be used for organizations such as het Rijk, municipalities, provinces and waterboards (Bio-overheid, 2020). The BIO is designed because information security forms an important quality aspect in providing information from governments to public. Moreover, the

BIO aims at assisting management with taking responsibility regarding information security and attempts to simplify risk management. The BIO provides standardized basis security levels (BBN's) (standaard basis beveiligingsniveau's) together defined with the belonging protection requirements per BBN. Furthermore, the BIO supplies management with the least requirement controls from the ISO 27002 per BBN, while controls are also defined in obligated requirements to simplify decision making and responsibilities for management. Moreover, management must provide responsibility about the decisions and considerations made in how controls from the BIO are fulfilled or being fulfilled. In conclusion, the main focus of the BIO is to provide all governmental organizations and institutions a basic principal guideline on how to improve protection and security of all information(systems) on and within every unit needed (Bio-overheid, 2020).

In addition, Pilorgett and Schell (2018) state that IT activities within an organization requires a certain balance within the organization. Besides, Pilorgett and Schell (2018) point out that organizations have a need of a functioning of IT roles and at the same time have a certain effect on the IT process. This means that governance components are embodied by the organization as a whole. The degree in which IT and business areas, combined with degree of integration of IT processes influences the maturity of the IT process and therefore at the same time influences the maturity of the information security practices. Hence, it is important to take explore maturity in the context of processes within businesses, for both the private sector and more importantly the public sector.

2.3 Tools for growth and maturity measurement

In order to measure growth, the concept of maturity is taken into account during the process of research for the measurement of growth. Cook-Davies (2004) suggests that there is no commonly agreed definition of what a mature project-based organization looks like. Wendler (2012) finds it interesting that a definition of the term of maturity model is often avoided, research mostly makes use of descriptions and functioning. Klimko (2001) for example, defines maturity models as models that provide a description of development of an entity over time. Moreover, Klimko (2001) states that entities can be anything, such as human beings or organizational functions. However, maturity models are considered known tools used for rating capabilities within domains, for guidance of organizations and decision making of actions needed towards achieving higher levels of maturity (Kohlegger, 2009). Additionally, Becker (2009) claims that maturity models are considered valuable tools for (IT) managers because current and desirable situations about different domains, processes and procedures can be assessed. Accordingly, maturity models in information security practices can be of help in assessing the capabilities, strengths, weaknesses and areas to improve of organizations in achieving the obtained security goals (Saleh, Information security maturity model., 2011). Moreover, the first influential theoretical model with a main focus on a combination of growth and stages, for the field of information systems was developed by Richard Nolan: The Stages of Growth Model (King, 1984). The model was introduced at first, containing four stages: initiation, contagion, control and integration. The other stages; integration, data administration and maturity were added later. The first three stages have a strong aim towards technology while the last three stages are aimed towards management of technology (Duane, 2012).

In addition, within the field of information security in this research, the models that will be further explored are the Capability Maturity Model, the NBA Maturity Model proposed by the Royal Dutch Organization for Accountants, the Information Security Maturity Model, Cybersecurity Capability Maturity Model and the Capability Maturity Model and metrics framework for Cyber Cloud Security. These models are considered important within this case of research because all of them are related to the topic of information security and some of them even to each other. All have similarities and form the basis for one and the other which is common in maturity model development in general (Wendler, 2012).

Capability Maturity Model

After further development and revision of growth models, Paulk et al. (1993) introduced the Capability Maturity Model Integration (CMMI) initially based on the improvement of software processes. The CMM, refer to Appendix I for a visual description, as proposed by Paulk et al. (1993) identifies the goal of the CMMI, as the goal to reach a certain level of maturity. Moreover, Paulk et al. (1993) highlights the difference between organizations that are mature and immature as followed: *"In an immature organization, software processes are generally improvised by practioners and their managers during a project. Even if a process has been* *specified, it is not rigorously followed or enforced"* (p. 19) and *"a mature organization possesses an organization-wide ability to manage development and maintenance. Managers communicate accurately the process to staff and new employees, and activities are carried out according to the planned process."* (p. 19). Moreover, Paulk et al. (1993) define five distinctive maturity levels, where achieving every level of maturity within the model results in increasement of process capability of the organization on which it is applied. Moreover, every level is dependent from the previous one and each one is set up as a basis for the following one. The five levels of maturity are described and listed as (Paulk et al., 1993):

- *Level 1:* Initial: at this level, an organization does not provide an environment that is stable enough for the development and maintenance of processes of software. Organizations at this level often have difficulties making commitments that staff can meet with an orderly engineering process, resulting in a crisis. During a crisis, projects typically abandon planned procedures and revert to coding and testing. Success depends entirely on having an exceptional manager and a seasoned and effective development team. Occasionally, capable and forceful managers can withstand the pressures to take shortcuts, but when they leave the project, their stabilizing influence leaves with them. Even a strong engineering process cannot overcome the unstableness created by the absence of management practices. Moreover, focus is not pointed towards the organization, but on individual and is characterized by this in capability as well. Capability becomes a trait of the individual and not of the organization (Paulk, 1993).
- *Level 2:* Repeatable, this level is characterized by implementation of policies for management and establishment of implementation of procedures. Experiences with alike projects are the basis of planning and management of new projects. Moreover, capability of processes are enhanced by imposing management disciplines, while there is clear definition of project standards while the organization creates an environment where processes can be followed. This level is characterized by the discipline of organizations due to neat project planning and tracking based on earlier success.
- *Level 3:* Defined, this level is characterized by the process of development and maintenance of processes, documented across the organization. Additionally, together with engineering and management processes which integrated into the

whole. Both of these processes are stable and repeatable in this capability level and understanding of activities, roles and responsibility is defined across the organization.

- *Level 4:* Managed, this level is achieved when the organization has set quantitative quality goals for products, as well as processes with well-defined and consistent measurements. Databases that collect data on an organization-wide level, collects data that is needed for analysis of the particular process. This level of maturity enables an organization to be able to predict trends in processes and product quality. Since the process is accurately measured and stable at the same time, unexpected occurring circumstances can be identified and address the event. When acknowledged limits are overtaken, managers are able to take correct action in repairing situations.
- *Level 5:* Optimizing, this level is achieved when the organization as a whole has focus on continuous improvement. The goal is proactively identification of weaknesses and strengthening of the processes while the main target is to prevent defects in the selected process. Organizations that find themselves at this level use data on process effectiveness to perform analyses and come up with new techniques of changing processes. This level concludes by stating that waste is unacceptable and that reducing waste is the main focus of level 5.

The CMMI is mostly applied in software development areas and can be applied and used by different sort of organizations like software- and system engineering firms. Companies that act at a level 1 stage are mostly start-ups without real documentation of processes and execution. Companies that act at level 5 are organizations that have a well-defined and formalized processes that are therefore able to be in search for optimization of these processes. Level 5 type of organizations are mostly corporate organizations that are aware of risks and dangers of this field.

Moreover, within the scope of this research, since it's focus is on Dutch Public Organizations, there are also other developed maturity models pointed towards these type of organizations, which need further clarification.

NBA Maturity model

In May 2019, the Royal Dutch Organization for Accountants (Koninklijke Nederlandse Beroepsorganisatie van Accountants: NBA) developed and proposed an official maturity model for information security translated into a practical model (NBA, 2021). Moreover, this model shows similarities with the above mentioned CMM model within the fundamental of the model. The reason for developing such maturity model comes from the persistent challenge of improving (maturity) of information security within organizations, while the minimal improvements that are realized, are mostly on small sections and departments in organizations while there is need of company-wide improvement. Besides, targets for improvements are not taken into account in the organizations plans and not visible in budgets, as is experienced by accountancy organizations in the Netherlands (NBA, 2021). The initial edition of this model has even been used before the official announcement in 2019. During plans of the ministry of Justice and Safety in 2018, for a plan of approach in improvement of information security for this ministry, after collaboration between NBA and the Dutch Order of Registered EDP-auditors (Nederlandse Orde van Register EDP-Auditors: NOREA) the official model was announced.

Moreover, the model needs detailed input from the organization in different forms about several elements. First of all, as an example: input is needed about the area of attention in which the model needs to perform, while the model separates fifteen different area's like governance, IT, HR, data management and many others. Moreover, as an example the model asks for a description of the risk that is consequently visible when the control measure is not effective. Furthermore, the model asks for a indicative maturity level as well.

In the end the model gives an end score of 1 to 5 with a description based on the input, that is answered in the different sections at the beginning of the model.

- *Score 1:* Initial: Control measures are not, perhaps partly defined and are performed in an inconsistent way. There is big dependence of individual factors.
- *Score 2:* Repeatable: Control measures are present and are being performed consistently and structured. However, performance is in an informal way.

- *Score 3:* Defined: Control measures are documented and are being performed in a structured and formal way. Fulfilment of these measures is verifiable and is being assessed.
- *Score 4:* Controlled and measurable: Effect of control measures is being evaluated periodical.
- *Score 5:* Continual improvement: The control measures are fiercely established in the documentation of risk management of the organization while there is the continual hunt for improvement.

Information Security Maturity Model (ISMM)

Another maturity model is the Information Security Maturity Model (ISMM) as developed by Saleh (2011), refer to Appendix I for a visual presentation, is proposed as a model to build-in the security in an organization and to evaluate abilities of organization to meet the intended objectives from the CIA triangle.

Additionally, the ISMM model is designed containing four overlapping basis domains which are organization governance, organizational culture, architecture of systems and service management. Moreover, the ISMM is focused on levels of compliance. Since Saleh (2011) beliefs that security is to improve as the selected organization is able to improve around the compliance levels:

- Non Compliance: This first phase of the ISMM is defined by the lack of existing policies and procedures around security of the core business. Moreover, it is characterized by the lack of consideration of investments in systems related to security. Finally, organizations do not even consider to estimate the effect of vulnerability and do not bother to value the risks coming along as a result of the vulnerabilities.
- Initial Compliance: The second phase of the ISMM is characterized by the first point of the fact that an organization is aware of threats around the security subject. Additionally, the initial compliance phase is defined by chaos, inconsistency, ad hoc and being respondent to attacks as a result of loss of resources after attacks. This phase is also defined by the lack of designed policies or procedures in order of protection of systems within the organization. This phase is also characterized by small practical implementations in systems. However, in a reactive way.

- Basic Compliance: This phase of the ISMM can be considered as the least compliant an organization needs to be when there is a need for protection of investment and assure continuity of systems. This phase is defined by the present security of applications and network without central management of this protection. There is a strong belief in interaction between users and applications or systems. Moreover, security procedures not formally defined and there is very few assessing of risks.
- Acceptable Compliance: The fourth phase of the ISMM is defined by the presence of centrally managed security and policy around this subject. This phase is characterized by the belief that users of the system and especially their action executed in applications and within the network are considered vulnerable for security of the organization. Next to that, there is a strong presence of ownerships around security measures and there are formalized policies around compliance of information security measures. Moreover, there is a strong drive to raise awareness among the organization for these kind of topics.
- Full Compliance: The final stage of the ISMM is defined by the control the organization has over the security necessities. Moreover, systems are being monitored, the organization is conscious of threats and there is a constant comparison to international standards. This phase is also characterized by the formal policies and procedures that are implemented in order to be able to prevent, but also adequately detect and correct matter around security. Next to that, this final stage of the model is also aware of the need of security architecture within the organization, there is a system that is able to track incidents and even track the status of every matter.

Cybersecurity Capability Maturity Model (C2M2)

Another model which is known in literature around the combination of information security and maturity models is the Cybersecurity Capability Maturity Model (C2M2), refer to Appendix I for a visual description. This is a maturity model which is proposed by the Department of Energy of the United States. Moreover, the model categorizes in four different maturity stages: no practices, initial practices, stable practices and practices stabilized. This maturity model is known for the combination of already existent security standards to assist in development of security capabilities of the organization (Stoneburner, 2002). Moreover, the C2M2 model is usable for different organizations from all sizes because of the way of presentation since it contains a high level of abstraction. The model is classified into ten different so called domains, grouped in security practices. The first domain is Risk Management, the second is Asset, Change and Configuration Management, the third is Identity and Access Management, the fourth is Threat and Vulnerability Management, the fifth is Situational Awareness, the sixth is Information Sharing and Communications, the seventh is Event and Incident Response, Continuity of Operations, the eighth is Supply Chain and External Dependencies Management, the ninth is Workforce Management and the last one is Cybersecurity Program Management.

Capability Maturity Model and metrics framework for Cyber Cloud Security (CMMCCS)

The last maturity model selected is the Capability Maturity Model and metrics framework for Cyber Cloud Security (CMMCCS) as proposed by Le and Hoang (2017), refer to Appendix I for a visual presentation. The model as proposed has a focus on cybersecurity matters and cloud computing. The model is developed in order to contribute to the direction of organizations in supporting them in implementation of the improvement of cyber security capabilities around cloud systems. The model is shaped around twelve different domains: Governance, Risk, and Compliance management, Audit and Accountability, Identities and Access Management, Data and Information protection, Incident response, Infrastructure and facilities security, Human resource management, Security awareness and training, Cloud application security, Virtualization and isolation, Interoperability and portability, and finally Cloud connections and communication security. Moreover, the model is categorized into four different stages that start with level 0 and finish at level 3.

The table below lists the characteristics of the selected models.

Table 1: Similarities and differences between maturity models

NBA Maturity model	**Capability Maturity Model Integration (CMMI)**	**Cybersecurity Capability Maturity Model (C2M2)**	**Information Security Maturity Model (ISMM)**	**Capability Maturity Model for Cyber Cloud Security (CMMCCS)**
Scale of scores from 1 to 5	Scale of scores from 1 to 5	Scale of scores from 1 to 4	Scale of scores from 1 to 5 (not in numbers)	Scale of scores from 0 to 3
Division of levels: Initial, Repeatable, Defined, Controlled and Measurable, Continual improvement	Division of levels: Initial, Repeatable, Defined, Managed, Optimized	Division of levels: No Practices, Initial Practices, Stable Practices, Practices Stabilized	Division of levels: Non-Compliance, Initial Compliance, Basic Compliance, Acceptable Compliance, Full Compliance	No further description of scores
Focused specifically on information security	Focused on software processes	Focused on cybersecurity	Focused specifically on information security	Focus on cybersecurity cloud computing
Each level is dependent of the previous one	Each level is dependent of the previous one	Each level is dependent of the previous one	Each level is dependent of the previous one	
Needs input from different perspectives within the organization	Basic model which forms foundation for a lot of models	Focus on ten different domains and therefore usable in different contexts of organizations	Based on four different domains: organization governance, organizational culture, architecture of systems and service management	Based on twelve different domains

As can be seen in all maturity models, there is significant similarity in the basis of the maturity models. Out of the selected maturity models, there are three that make a distinguishment between five stages and have a last stage that is mostly focused on the improvement of the subject the model is about. While the other two have scores which are scaled into four different categories. Additionally, it is visual that all models have an overlapping focus on elements within organization, while one is a bit more specialized than the other.

3. Methodology

This chapter defines in depth how this study was conducted, i.e. the methodology of this research. Therefore, a further and in-depth explanation will also be given about the conceptual research model. Moreover, reasons for selection of certain use of methodology will be further clarified.

3.1 Research design

Since the goal of this research is to examine and conclude why Dutch Public Organizations fail to achieve higher levels in information security and what could drive and encourage Dutch Public Organizations in their approach towards information security, it is important to determine a set of research questions in guidance towards a conclusion on what Company X and Dutch Public Organizations needs to act upon in increasement of maturity.

3.2 Research model

Based on elements that are considered in this research, a research model is created, shown in Figure 2. First of all, this research model shows the subject which the research is about: Dutch public sector organizations. Secondly, the goal that is intended to achieve is made visible through an arrow that is pointed towards the right side, which is maturity in information security. Additionally, factors that enable growth and factors that can increase or even decrease or hinder growth in information security are added at the top and bottom of the research model.

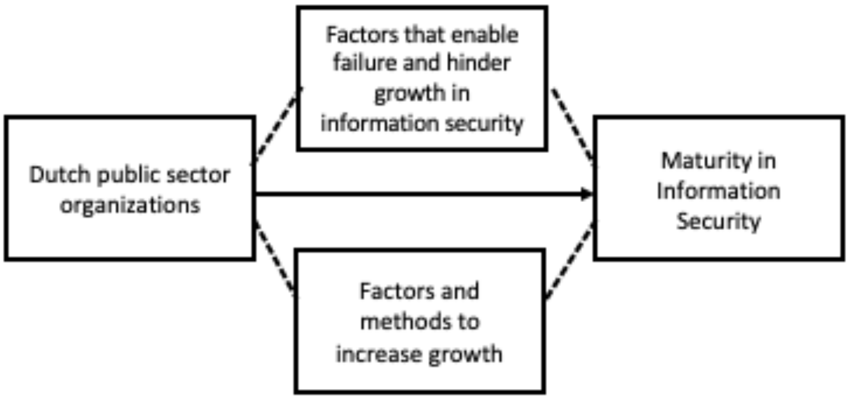

Factors that enable failure and hinder growth in information security
Dutch public sector organizations
Maturity in Information Security
Factors and methods to increase growth

Figure 2: Conceptual research model

3.3 Scope and sample

To not further broaden the scope of this research, it is of importance to focus generally on a specific type of user and usage. Previous research about implementation of BIO within Dutch Public Organizations (municipalities and waterboards) proposed that further research could be done with a focus on ‘bigger organizations in the public sector’ (Somers, 2021). Bigger can be interpreted in different ways, since inhabitants of a municipality can be taking into account, employees within organizations or even employees within the organizations that are concerned with the topic or task of information security. Therefore it is decided to solely focus on organizations within the Dutch public sector, in form of municipalities, preferably related to Company X. Additionally, the aim is to conduct research on Dutch Public Organizations, more specific municipalities that have at least 50.000 inhabitants because it is expected that this relates to staff members and therefore complexity within the organization. However, for this reason it must be kept in mind that this limits further and future conclusions and generality of conclusions of this research.

3.4 Type of research

In research, the most generally known types of conducting research are quantitative and qualitative research. During the fulfilment of qualitative type of research, the main goal is to explore and recognize the reasons of behaviour towards a problem or situation. This type of research is in need of (sub)questions to be able to provide a meaningful conclusion to the research that needs to be done. For this reason, qualitative research is about reasoning through an inductive manner, this form of reasoning suggests providing evidence for a conclusion that is made and attempts to generalize the observed answers and results of research (Creswell, 2016). Since type of research is mostly depending on the goal of research and the research question of the study, these are important factors to take into consideration in decision making of type of research. Since this research attempts to gather information and insights in why Dutch Public Organizations fail in achieving sufficient levels in protection and security of information, this research can be considered exploratory and therefore the method of qualitative research will be applied during this research. Moreover, since even responsible governmental organizations that develop regulations, experience hardship in setting right thresholds of minimum achieved levels and even the BIO itself does not mention a level that should be achieved at least. Nevertheless, the IBD for example, in their GDPR guarantee product 2.0 (AVG Borgingsproduct 2.0) points out that level 3 is the least minimum level an organization should achieve around GDPR measurements (IBD, 2021). Therefore, this research aims at level 3 as a minimal and sufficient level as well, since these practices are closely related.

3.5 Research method and data collection

During the process of qualitative research, the use of two sorts of interviews are commonly used: semi-structured and unstructured. Interviews during the fulfilment of qualitative research lack structure but at the same time provide flexibility since the researcher can depart from schedules and attempt to gather answers which are detailed and more precise (Bryman, 2016). Since this research seeks for the main reasons and factors why Dutch Public Organizations fail in maintaining and achieving a sufficient level of information security and tries to examine what drives them in order to achieve higher levels, one of these types of interviews seems suitable. Therefore, semi-structured interviews with stakeholders such as IT auditors, IT advisors and Dutch Public Organizations probably makes the best fit for this type of research, since this type of interview enables the researcher to challenge the respondent to provide answers as detailed as possible. Moreover, the researcher can follow up on questions and answers moreover, to gather in depth answers as well. Interviews that are follow a strict structure or pattern would prevent the researcher of deepening into subjects and topics during the assessment of the interview.

In order of limiting biases as much as possible, respondents need to be carefully selected (Bryman, 2016). Since the topic of this research is not generally known, respondents need to be somehow related to the topic of research. Therefore, it is important to select experienced IT auditors and IT advisors currently involved in this topic to collect answers and results that are result of high level of knowledge on the topic of information security within Dutch Public Organizations. Respondents can be chosen based on certain criteria, such as: respondent needs to be affiliated to Company X as an employee within the IT Advisory department, preferred to be an advisor or auditor because of expected high level of knowledge and expertise, respondent needs to be connected to Company X as a client, preferred are contacts such as CISO's, since such type of roles are mostly concerned with the topic of research. The most important element of interviewing IT advisors as well as CISO's from Dutch Public Organizations is because the main goal is to gather information from both sides around the process. IT advisors and auditors can tell about their experiences and observations from the perspective of an advisory firm. While CISO's can provide insights in what their experiences are towards the activities of IT advisors and auditors. Furthermore, these respondents can also provide insight in what the main reasons are for the failure of achieving intended information security levels. Moreover, CISO's can also give more insight in what their experiences are towards rules and regulations, frameworks and models used in literature and their own field of work.

With regards to data collection, the element of theoretical saturation must be kept in mind. Theoretical saturation refers to the data collection until there is no new generation of insights, that is the point where the researcher has gathered sufficient amount evidence for observations (Bloor, 2006).

3.6 Reliability and validity

In order to conduct research, it is important that this research is valid and reliable. Reliability of research refers to repeatability of results and conclusions when research is conducted by different researchers. Reliability also refers to gathering answers when research is done by the same researcher but when research is done at another time and/or place. Research is considered reliable when in these situations, same results are obtained. Achievement of reliability is hard during execution of qualitative research since results could differ based on perception of the particular person who is doing research. Validity can refer to different forms of validity such as measurement validity, internal validity and external validity. Internal validity aims at the relationship between variables within research (Bryman, 2016). Since this research is set up in a qualitative design, measurement validity is not applicable while the same counts for internal validity because of the same reason regarding research design in a qualitative way. External validity is more about findings of research and if these are able to use in a general way (Bryman, 2016). Interviews will attempted to be done with experienced IT advisors and/or auditors, with CISO's and other possible employees from Dutch Public Organizations that are involved in information security matters. Moreover, the Dutch Public Organizations will be limited to organizations, served by Company X, such as municipalities with at least 50.000

inhabitants. This means that external validity can be judged as limited somehow because conclusions of research are applicable on a limited group of respondents.

3.7 Analysis

Data that is gathered and collected through qualitative manners such as interviews, requires sufficient analysis. One of the ways to analyze qualitative data is called Thematic Content Analysis (TCA), which is a representation of qualitative data that is presented in a descriptive way (Anderson, 2007). Moreover, TCA can be used on different forms of data like video, sound, but most important on data in form of text such as interview transcripts.

An important step in TCA is coding, which even forms the starting point in the analysis of data. Charmaz (2006) claims that coding of data is an important and first step in performance of analytical interpretations after concrete statements.

Analysis starts with coding of information, which has multiple goals and functions according to Boeije (2009); coding is important for data management since information is organized and categorized. Moreover, through coding of the data, data is explored and interpreted. Lastly, through coding, data is put together in different forms to come to new perspectives regarding data gathered. Furthermore, Boeije (2009) argues that there are three main phases during the coding of data, which are:

- Open coding: this form of coding means that all collected data needs to be read thoroughly and needs further dividing in fragments. All fragments need to be compared to each other while the content needs categorization and labelling with a code. This phase of coding ends whenever there is no need of adding new codes anymore, this means that the phenomena of saturation appears, since all new elements in research can be divided in existing codes.
- Axial coding: this form of coding defines that data needs to be put together in new ways after open coding and implies that new connections need to be made between categories to decide about dominant elements in research. The main goals of this phase is to reduce and reorganize the data that is collected and to decide dominant elements in research. Axial coding separates codes from data, while in the first phase of open coding, data itself was the main point of focus.
- Selective coding: during the fulfilment of the last phase of coding, the researcher needs to find out what elements and theme's constantly return during observance of the

responses the researcher gets from respondents, which makes these elements the most important observation of all respondents observed. Through this phase of coding, the researcher identifies the relation of patterns during research and attempts to find out which core concepts can be regarded as most important results in research.

3.8 Exploratory interviews

Exploratory interviews were held in a semi-structured way with the following persons as can be seen in Table 2. These respondents were selected based on their experiences with Dutch Public Organizations and their information security practices within their function related to IT Advisory. Interview questions asked to respondents can be seen in appendix II. Moreover, Table 2 shows which person was interviewed, their role within the organization and date of interview.

Table 2: Exploratory interviews with Company X IT Advisory

#	Function/Role	Organization	Date
1	Senior Consultant IT Advisory	Accountancy firm	09-12-2021
2	Senior Consultant IT Advisory	Accountancy firm	21-12-2021
3	Senior Manager IT Advisory	Accountancy firm	22-12-2021

During the fulfilment of this research, Covid-19 regulations unfortunately were still applied to working environments, resulting in interviews conducted through Microsoft Teams. Fortunately, employees within Company X were used to online work environments in the meantime, meaning Microsoft Team meetings were recorded to listen to interviews at a later moment for transcribing interviews as well. All interviews with Company X employees are fulfilled in the same manner.

The questions asked during the interviews with Company X IT Advisory employees were sent in advance to respondents to get a view on what respondents could expect of the interview. Moreover, the questions were asked to understand the view of IT Advisory employees on information security practices within Dutch Public Organizations. The list of questions asked during these interviews can be found in Appendix II.

3.9 In-depth interviews

Several in-depth interviews were conducted with CISO's within the selected organizations. The intention of fulfilment of these interviews is to examine and understand what employees within Dutch Public Organizations bothers and to understand what their experiences are with information security related matters. Through these interviews, their view on these matters can be better understood and therefore find out what elements or factors hinders them in growing in information security practices. The list of questions asked during these interviews, are attached in Appendix III.

Employees of organizations that participated are listed in Table 3. These participants, all from unique organizations, are chosen on basis of their experience with information security practices and current roles within the selected organizations.

Table 3: In-depth interviews with organizations

#	Function	Organization	Employees	Date
1	Chief Information Security Officer	Municipality	1000	24-12-21
2	Team manager information and Support	Municipality	400	29-12-21
3	Chief Information Security Officer	Municipality	600	06-01-22
4	Information Security Officer	Municipality	800	10-01-22
5	Team manager information and Control	Municipality	400	11-01-22
6	Chief Information Security Officer	Municipality	500	12-01-22
7	Chief Information Security Officer	Municipality	750	14-01-22

During fulfilment of this research, Covid-19 regulations unfortunately were still active and applied to working environments. This resulted in interviews conducted through online channels like Microsoft Teams. Fortunately, respondents were used to online working environments in the meantime, meaning Microsoft Team meetings were recorded to listen to interviews at a later moment for transcribing interviews as well.

4. Results

This chapter provides an overview of the results that are collected during this research.. First of all, the results of the semi-structured exploratory interviews are briefly analyzed since these interviews form the input and determine a considerable part of the rest of the research and interviews with the respondents within Dutch Public Organizations. Furthermore, the results of the interviews with respondents within Dutch Public Organizations will be further analyzed as well. At last, a conclusion will be formed of the most significant results gathered.

4.1 Analysis of exploratory interviews

Table 4, which can be seen below, represents a structured analysis of results that are gathered during the interviews that are held with IT auditors and IT advisors. This section attempts to define the view of IT auditors and advisors on the current struggles that Dutch Public Organizations are dealing with and that disable intended growth. Moreover, the below mentioned factors are explained by examples and citations underneath Table 4: *Analysis of interviews with IT auditors and/or advisor*. The table is developed on basis of the interviews with IT auditors and advisors and consists of 7 main themes. These main themes are further divided and consist of 2 to 4 subthemes that come along with 1 to 3 citations of the different respondents to illustrate the main themes and subthemes. This build-up goes on as well with all main themes, which are: priorities, knowledge and expertise, frameworks, consequences, roles and responsibilities, awareness and culture and behaviour.

Priorities

The first main theme is ‘priorities’. Priorities relate to the opinion of the respondents that experience that the topic of information security is not on top of the priority lists within Dutch Public Organizations due to various reasons. This first main theme contains the following subthemes: setting priorities in general, amount of responsibilities that make it hard to set priorities and financial budget priorities. The first subtheme relates to the fact that respondents experience that Dutch Public Organizations have difficulties with setting priorities in general to change because of multiple reasons such as the fact that they are working like this for many years. This is illustrated by respondent #1 that emphasizes this through the following example: ‘Organizations are running like this for more than 40 years, what and where should they start with?' Moreover, about this, respondent #2 for example explains that the combination of time and setting priorities plays a role by pointing this simply out by stating: *'That's the word: priority! And a lack of time is a consequence of not setting the right priorities!'*. The second subtheme relates to the amount of responsibilities Dutch Public Organizations have which makes it hard to set the priorities in this topic of research and grow further in maturity in information security. About this, respondent #1 explained the situation as: *'When the mayor walks down the street, he probably will be approached about whole other stuff than information security matters, what about the parking lots?'.* Respondent #2 pointed out that information security matters have a low priority for managers and defined this as followed: *'The manager of the permission department is busy with handing out permits, the part in his job that is related to information security is bottom of the list'*. The last subtheme within the main theme of priorities is the relationship between setting the right priorities combined with financial budget choices that need to be made. About this, respondent #1 pointed out: *'Because they have much more responsibilities and they can only spend money once, it's hard to grow'*.

Knowledge and expertise

The second main theme is 'knowledge and expertise', this main theme mainly relates to the lack of knowledge and expertise within this field of research. This theme contains of three subthemes. The first subtheme relates to the fulfillment of function without the proper qualifications. Respondent argue that responsible (line)managers do not have sufficient knowledge about information security and therefore lack the proper qualifications to be able to convince their own staff to be more aware and learn them more about information security. About this, respondent #3 argues: *'CISO's are most of the time just system engineers without knowledge about the field of information security'*. The second subtheme is about the lack of knowledge about the topic and relates to the lack of knowledge within the rest of the organization with exception of CISO's. Respondents argue that other (lower management) levels within the organizations and other departments are not taught enough about this topic. About this, respondent #2 notes: *'A CISO probably knows about information security, but the rest of the organization does not, and those are the ones who need to get going'*. The last subtheme within the main theme of knowledge and expertise is related to the BIO.

Respondents are convinced that the lack of sufficient knowledge about the BIO among management makes them unable to further spread it over the organization and therefore plays a role in not further growing within this topic of research. Respondent #2 elaborates on this as: *‘Management maybe only heard about it, the rest of the organization didn’t and doesn’t know about it’*.

Frameworks

Another considered main theme that ensures organizations to not further grow in information security practices is ‘frameworks’. This main theme contains of one subtheme and refers to the usage of frameworks in evaluation and monitoring. The participating respondents in the form of IT auditors and/or advisors argue that organizations need to make more use of control frameworks that ensure more monitoring and evaluation in the form of PDCA cycles for example. About this, respondent #2 argues: *‘Organizations have a certain limited basis, but to what extent are they also applying control cycles?’* and respondent #1 is strongly convinced that there is no evaluation process, therefore respondent #1 claims: ‘*Plan and Do is done, but Check and Act is forgotten about’* and at the same time, respondent #3 claims: *‘They have some information security measures, but do they evaluate them periodically? No’*

Consequences

The fourth main theme is ‘consequences’ and consists of two subthemes. The first subtheme is described as the lack of consequences. This relates to the belief of the respondents that the lack of ‘real’ consequences of not being BIO compliant for example, enables organizations to not further pursue development to higher levels in maturity. With regards to this, respondent #2 elaborated: *‘There are no real consequences when organizations don’t comply, there are just risks in practice for them’*. Moreover, respondent #1 pointed out that organizations need to feel fear: *‘Organizations need to feel the fear and be scared in order to get them going and moving for us’*. The second and last subtheme within the main theme of consequences relates to consequences in a political way that need to push organizations to further develop in this field of research. Respondent #2 argues: *‘If you don’t do things the right way, within the public sector, the media jumps on it and a mayor who is not an expert can answer the media’*.

Roles and responsibilities

The next main theme is described as 'roles and responsibilities' and contains three subthemes. According to the participating respondents, growth in information security is disabled through the lack of division of roles and responsibilities. The respondents experience that organizations find it hard to grow in information security because there is no clear distribution of roles and responsibilities regarding the information security practices within municipalities. The experiences of participating respondents around the division of roles and responsibilities variate. Therefore there are three subthemes that variate from taking responsibility in general, taking ownership in information security practices and the lack of formalized division of these roles and responsibilities. The first subtheme is therefore described as 'taking responsibility' and is being elaborated by respondent #1 as: '*When responsible people take ownership in their role, the rest of the organization, underneath them, is ready to work on and for it'*. The following subtheme is 'ownership' and refers to the lack of ownership that is taken by managers, but that should be taking this ownership within this field of research. Respondent #2 notes: *'In order to be BIO compliant, you need to have a PDCA cycle. But therefore you need someone to stand up and take ownership!'* and respondent #2 also notes that managers do not realize what their responsibility is in this field of research: *'Not everything is the responsibility of the CISO, when something goes wrong, it's the responsibility of that specific manager that can't do his or her work anymore'*. The third subtheme is about the lack of clear division in these roles and responsibilities. According to the respondents, this relates to the sense or feelings of responsibility towards information security practices. Respondent #2 points out that he experiences that people, most especially managers, within municipalities always think that every information security related matter is the responsibility of the CISO or an IT related department: *'There is still an image that every information security matter is the responsibility of the CISO'* and *'When a manager uses an application, he just thinks that the IT department is responsible for it and will take care of the problem'*.

Awareness

According to respondents, another factor which can be considered as a main theme is 'awareness'. This main theme is further specified into one subtheme as 'factors increasing awareness and pressure within organizations'. This relates to the feeling that respondents have that internal and external pressure can increase awareness to further develop information security practices and achieve higher levels of maturity along as well.

This form of internal pressure can be from a person that has a role in development of information security practices or from incidents that occur within other organizations like a hacking. Respondent #1 for example claims: *'They get going when there is pressure. From outside because it's obligatory. When something happens elsewhere, like a hacking. Or whenever a CISO takes ownership and is able to spread it over the whole organization'*. Respondent #2 highlights the importance of external pressure and for example states that incidents that occur at other municipalities help in raising awareness again: *'Those are the cases that help regain focus and make organizations ask themselves: are we on the right track?'*.

Culture and behavior

The last considered main theme is 'culture and behavior' and refers to the belief of the respondents that the culture within an organization and the behavior of, and among employees plays a role in growth in information security. This main theme is divided in four subthemes: purchase management, supply management, risk management and change management. These subthemes mainly relate to the belief of the respondents that argue that certain processes within organizations are not sufficiently designed to be able to grow in this topic of research. The first subtheme, purchase management, is being categorized and referred to, because respondents are convinced that information security is often forgotten about when new applications or systems are being bought, respondent #1 argues that: *'A CISO should also be in charge when new applications are bought, to consider all information security measures as well'*. The second subtheme of supply management refers to the importance of compliance of suppliers with information security measures. Respondent #1 for example describes the location of hosting of applications as one of the elements: *'CISO's also need to check where an applications server is running, and what SLA's are applied'*. Respondent #2 points out that it's useless to be compliant when suppliers are not: *'You can comply, but it's useless when your suppliers are not complying to information security measures'*. Moreover, the third subtheme relates to risk management which is not sufficiently present in processes and behavior to be able to grow further, according to the respondents. Respondent #2 states: *'They don't see the profit and see it as annoyance instead, but it's all about risks in the* *organization, that's what they need to see'*. Respondent #3 describes this as: *'People need to consider the risks about measures, it's something you need to decide about to grow and get your levels sufficiently'*. The last subtheme is change management which disables people in organizations and therefore the organization itself, to grow further. Respondent #1 for example states this as: *'The most difficult part is to get the people in the organization moving, I call them the line managers, they must understand that they are the ones who need to get going!'*.

Table 4: *Analysis of interviews with IT auditors and/or advisors*

Category	**Description**	**Example quote**
Priorities	Setting priorities in general	*'A municipality cannot prioritize everything!'*
		'Organizations are running like this for more than 40 years, what and where should they start with?'
		'That's the word: priority! And a lack of time is a consequence of not setting the right priorities!'
	Amount of responsibilities that make it hard to set priorities	*'It's not weird, a municipality has so many responsibilities, resulting in so many different processes and systems'*
		'Municipalities have so many obligations, they sometimes unconsciously give priorities to other things because they simply can't prioritize everything at the same time'
		'When the mayor walks down the street, he probably will be approached about whole other stuff than information security matters, what about the parking lots?'
		'Manager of the permission department is busy with handing out permits, the part in his job that is related to information security is bottom of the list'
	Financial budget priorities	*'They can only spend their money once'*
Knowledge and expertise	Fulfillment of function or role without proper qualifications	*'CISO's are most of the time just system engineers without knowledge about the field of information security'*
	Lack of knowledge about topic (with exception of CISO's)	*'Awareness is increasing, but people are still unknowing in this topic'*
		'A CISO probably knows about information security, but the rest of the organization does not and those are the ones who need to get going'
	Lack of knowledge about BIO	*'Management maybe only heard about it, the rest of the organization didn't and doesn't know about it'*
Frameworks	Lack of usage of control frameworks that ensure monitoring and evaluation	*'Organizations have a certain limited basis, but to what extent are they also applying control cycles?'*
		'Plan and Do is done, but Check and Act is forgotten about'
		'They have some information security measures, but do they evaluate them periodically? No'
Consequences	Lack of consequences	*'There are no real consequences when organizations don't comply, there are just risks in practice for them'*
		'Organizations need to feel the fear and be scared in order to get them going and moving for us'
	Political consequences	*'If you don't do things the right way, within the public sector the media jumps on it and a mayor who is not an expert can answer the media'*
Roles and responsibilities	Taking responsibility	'*When responsible people take ownership in their role, the rest of the organization, underneath them, is ready to work on and for it'*
	Ownership	*'Not everything is the responsibility of the CISO, when something goes wrong, it's the responsibility of that specific manager that can't do his or her work anymore'*
		'In order to be BIO compliant, you need to have a PDCA cycle. But therefore you need someone to stand up and take ownership!'
	Clear division of roles and responsibilities	*'When a manager uses an application, he just thinks that the IT department is responsible for it and will take care of the problem'*
		'There is still an image that every information security matter is the responsibility of the CISO, while they need to realize that when things go wrong, they are the one with the problems'
Awareness	Factors increasing awareness and pressure within organizations	*'They get going when there is pressure. From outside because it's obligatory. When something happens elsewhere, like a hacking. Or whenever a CISO takes ownership and is able to spread it over the whole organization'*
		'Those are the cases that help regain focus and make organizations ask themselves: are we on the right track?'
Culture and behavior	Purchase management	*'A CISO should also be in charge when new applications are bought, to consider all information security measures as well'*
		'What you often see is that information security is forgotten about when new systems or applications are being bought'
	Supply management	*'CISO's also need to check where an applications server is running, and what SLA's are applied'*
		'You can comply, but it's useless when your suppliers are not complying to information security measures'
	Risk management	*'They don't see the profit and see it as annoyance instead, but it's all about risks in the organization, that's what they need to see'*
		'People need to consider the risks about measures, it's something you need to decide about to grow and get your levels sufficiently'
	Change management	*'The most difficult part is to get the people in the organization moving, I call them the line managers, they must understand that they are the ones who need to get going!'*

4.2 Analysis of in-depth interviews

Table 5, which can be seen below represents the structured analysis of results that are collected through the interviews that are held with participating respondents from the different Dutch Public Organizations. This section attempts to define the view of the experts within the Dutch Public Organizations. These factors can be factors of positivity which enable improvement in maturity or factors that hinder the organizations and affect them negatively. The table is developed on basis of the interviews with the respondents from the different and unique Dutch Public Organizations and consists of 11 main themes. These main themes are further divided and consist to 6 subthemes that come along with 1 to 5 citations of the different respondents to illustrate the main themes and subthemes. This goes on for all main themes, which are: priorities, time, capacity, resources, awareness, responsibility and roles, frameworks, knowledge, maturity models, culture and behavior and accountant.

Priorities

The first main theme is 'priorities'. Priorities relate to the observed answers that respondents gave in how they experience that is hard to make information security a priority within the organizations and more specifically: the ability of setting priorities. This is due to different reasons, which are translated into the two following subthemes: focus is on the many processes and tasks and the newness of related tasks and procedures. The first subtheme relates to the fact that respondents belief that Dutch Public Organizations already have many processes and many different tasks which makes it hard to also find a way to prioritize the topic of information security. This is illustrated by respondent #1 which declared: *'As municipalities we have many tasks and responsibilities, so many processes, information security is often forgotten about and they don't feel the urge to handle this topic'*. Moreover, the second subtheme has to do with this new field of research. This outflows from the fact that, according to the respondents, information security related designs and processes are relatively new for organizations and their employees. About this, respondent #1 points out: *'Governance needs to be implemented, but municipalities never did something like this, why would they do it now? It's hard to get these things executed because it's not their priority'*.

Time

The second main theme is considered 'time' and is categorized into one subtheme: rules and regulations with regards to decision making. This relates to the hinder that organizations experience from all the rules and regulations that Dutch Public Organizations are bound to and need to follow. A participating respondent argues that their organization finds it hard to attract the right people because of all the rules they need to follow before an employee can be hired. The comparison is made with a profit organization that can hire someone and have them on board in a couple of days if needed. About this, respondent #2 notes: *'As a municipality we are bound to so many rules before we can decide about something. If a profit organization needs a new employee for a certain department or task, he could be sitting there tomorrow'*.

Capacity

The next main theme is described as 'capacity' and is further categorized into three subthemes. According to the respondents, this main theme hinders organizations in different forms such as capacity in forms of staff and employees, which relates to the lack of (skilled and experienced) right people. Respondent #3, a CISO for example, points out that lack of capacity in staff hinders the organization and that the organization is now busy looking for more people: '*We want to expand the team because we need more capacity to keep things safe, to react on incidents, we simply don't have that capacity now'*. Respondent #7 for example, elaborates on the fact that in the end after all the processes are designed in the right way, you still need enough and the right people to do the job: '*You can have plans and policies and stuff, but if you don't have the right people for the job? The right people to execute the projects. Else, you can put the plans back in the closet again. We are very busy now with searching for a good ISO for example'*. Moreover, the second subtheme is capacity in time which refers to the time that organizations do not have to keep themselves busy with information security regulations and further evaluate earlier taken measures around information security practices. About this, respondent #7 points out: *'There is simply no time to do such things like evaluation or anything, in municipalities we often work and live by what the day brings us and people are already busy with that'*. Additionally, respondent #3 argues that municipalities have too many applications and lack time to be in control of all of them:

'We have more than 400 applications, if you want to be in control of all of them, you need time'. The third subtheme is described as the lack of capacity in knowledge and expertise that leads to pushing off related tasks to information security. About this, respondent #1 argues that managers who do not have sufficient knowledge and expertise about the topic of research, are easier in pushing away the tasks and responsibilities that come along: *'Because managers think they don't have enough knowledge about the topic, they think they can just push it away'*.

Resources

Another considered factor which enables Dutch Public Organizations to achieve higher maturity is described as the main theme of 'resources'. This main theme is further described into one subtheme as the ability to attract right resources in staff. This relates to the doubt that respondents have, whether municipalities with all the rules they are bound to, are able to attract the right, experienced and skilled people. Respondents doubts if municipalities (especially that do not belong to the bigger municipalities) are attractive enough to work for, with the salary they can offer compared to other organizations. Other organizations in size, such as big municipalities, but also other profit organizations. Respondent #2 points out: '*I wonder if we are even able to attract the right expertise as a municipality, are we able to offer the right people the salary they can earn elsewhere?'*

Awareness

Another factor that the participating respondents experience as a variable that has an impact on growth is described as the main theme of 'awareness'. This relates to the awareness of staff, most especially operational staff. The participating respondents declare to still have a hard time in increasing awareness around the topic of research, although there is improvement. Moreover, current Covid-19 measures that are still applied and are translated to home offices do not make this job any easier. This main theme is further categorized into six subthemes. The first subtheme is called: knowledge because of recent implemented regulations. This subtheme is related to the belief of participating respondents that argue that the reason for being aware probably has to do with GDPR related measures that are applied in recent years, meaning that information security practices sounds relatively familiar and not completely unknown. Respondent #1 points out: '*GDPR related stuff is still fresh'*. The second subtheme is related to awareness due to previous external incidents. Respondents mention that incidents that occur at other organizations are helpful in a way that these incidents can raise awareness among own employees. Respondent #7 tells about this: *'The Hof van Twente case opened a lot of eyes and made them aware!'*. The third subtheme is more about the rising of awareness due to internal incidents. Respondent #3 even claims that internal incidents need to happen to raise awareness: *'As harsh as it sounds, an incident helps in raising awareness. People can get really upset when they cause something. Fortunately I never heard someone say that it's not a problem'*. The fourth subtheme is described as 'awareness programs' and is about the programs and forms of educations organizations have in order to raise awareness. Almost all participating respondents answer that their organizations have onboarding and different forms of e-learning programs to raise awareness among employees. Respondent #3 and #7 for example explain: *'Every new employee gets a basic training around the topic and we keep them updated through interesting e-learnings'*. Moreover, respondents also claim that awareness and keeping people motivated to handle this topic seriously is not a 'one time thing'. It is important to repeat and keep people interested. Respondent #4 and #3 for example point out: '*Repeating is the strongest message of advertising!'*. The fifth subtheme is about risks and underestimation. This is about people in Dutch Public Organizations that are not aware of risks and even underestimate the risks that come along information security practices. There is lack of realization that the size of a risk does not matter. Respondent #1 argues: '*They don't realize that a risk is still a risk, regardless of the size of it'*. The last subtheme is described as 'awareness by practice' and is about the belief of respondents that argue that it is important to be known in the organization for your role and responsibility you have as a CISO to make people aware. Respondent #4 argues that it is important to translate information security matters to people their own situations so that people understand better: *'By explaining, people understand, you have to make it practical so it becomes recognizable. People need to know you as well, so they know why and for what they are doing something. That's how you raise awareness and motivation'*.

Responsibility and roles

The next described main theme is 'responsibility and roles'. This is about the feeling of responsible behavior regards information security related tasks and division of roles in the processes that are related to information security. This main theme is further categorized into three subthemes: lack of feeling of responsibility, fear of responsibilities and lack of formalized procedures. The first subtheme is about the belief and experiences of respondents that managers, but also operational staff, believe that all tasks, procedures and processes related to information are the task and responsibility of teams that are related to IT for example. Respondents argue that these people do not feel the need to act responsible and take responsibility. Respondent #1 for example points out: *'As a CISO I have my responsibilities, the ISO has responsibilities, but the line managers need to know their responsibilities as well'*. Additionally, respondent #7 notes: *'They need to realize that information security is something for all of us, not only for a CISO'* and *'As a CISO I need to have a controlling and advising role, not an executing one'*. The second subtheme is more about the fear of responsibilities. Respondents claim that there is fear for accepting responsibilities and becoming officially process owners and accepting the responsibilities that come along. Respondent #1 for example argues: *'They know their role and responsibility, but don't want to have it written down, people don't want to have formal responsibility, they get scared'*. Another respondent argues that it is important to analyze risks with the process owner so that he/she understands and therefore can accept the responsibilities and the risks that come forth. Respondent #4 elaborates: *'When I do a risk analysis, I do that together with the process owner, so that he accepts the risks and the responsibility that comes with that'*. The last subtheme within this main theme is focused on the lack of formalized procedures. Several respondents also claim that organizations have no formalization of processes, meaning there are no formal process owners. However, respondent #7 argues that there is realization of process ownership and responsibilities: *'I think they know what their responsibility is, but we don't have it formalized. Yet! We are busy with formalizing it'*. Moreover, respondent #5 states: *'Things are being done for information security, but processes are not yet structured enough, there is no real description for every process'*.

Frameworks

The next described main theme is ‘frameworks’ and is categorized into two subthemes: lack of fulfilling monitoring frameworks and usage of ISMS. The first subtheme relates to when participating respondents were asked about the usage of certain frameworks or methods in policy development of information security, none of the participating respondents answered positive. There is no usage of such frameworks. It can be concluded that there is no fulfilment of a PDCA cycle for example. Frequently mentioned about this, is the lack of completing the cycle. This means that Plan and Do is done, without evaluation and monitoring through Check and Act. About this, respondent #6 points out: *‘We Plan and Do indeed, but we don’t Check and Act after implementation’*. However, the other subtheme is more about the respondents that answered positive on the method of managing information security developments through the use of Information Security Management Systems, some of them with a frequent usage, while some are not using it sufficiently yet. About this, respondent #3 for example points out: *‘We have it, but do not use it frequently enough yet’*. Whereas respondent #4 is in favor of using ISMS and develops improvement plans through the used ISMS and points out: *‘I use ISMS as some sort of PDCA cycle instead of tool. Through ISMS I can Plan, Do and evaluate to Check and Act!’*. Another element belonging to the usage of frameworks, is the lack of fulfilment of a PDCA cycle. Frequently mentioned about this, is the lack of completing the cycle. This means that Plan and Do is done, without evaluation and monitoring through Check and Act. Respondent #6 points about this: *‘We Plan and Do indeed, but we don’t Check and Act after implementation’*.

Knowledge

Another described main theme is ‘knowledge’ and is further specified into one subtheme which is described as: knowledge about BIO. This subtheme relates to the usage of the BIO and the knowledge of the BIO. Most respondents declared that operational staff is not familiar with the BIO. Participating respondents also state that it is not needed for operational staff, but only is discussed with management. Respondent #3 for example states: *‘The BIO is not clear for everybody. I never spoke to operational staff about BIO, only with the board and management’* while respondent #5 is not convinced about the added value to bother people in the organization because the BIO is too technical: *'The BIO is way too technical, I don't want to bother people with that'*.

Maturity models

Another categorized main theme according to the interviews with respondents is described as 'maturity models' and is further divided into four subthemes. The three subthemes are: usage of maturity models, limited knowledge about maturity models, lack of knowledge of maturity models and lack of realization of current levels. Usage of maturity models relates to the participating respondents that all answered negative when asked about their usage of maturity models in policy and policy making. With exception of respondent #7 who pointed out his knowledge and usage of the model: *'I know about CMMI, I even included it in our information security policy! But never heard of the other one'*. The second subtheme is about the limited knowledge that participating respondents have about maturity models. When participating respondents were asked about their knowledge about maturity models in general, almost all of them responded negative. There was no real knowledge about the CMMI maturity model, neither about the NBA model. About this, respondents answered: *'We don't really use them, but they can be a good guideline'*. The third subtheme is described as the lack of knowledge about maturity models and relates to respondents that never heard of these models. About this, respondents gave answers as: *'I don't know them that well, heard of it a few times'* and *'No, I haven't heard of them'*. The last subtheme can be considered more as a result of the previous subthemes, since there was limited knowledge and usage of maturity models, organizations were not able to make an estimation of their current maturity levels. About this, respondent #5 pointed out: '*Because I don't know them and never used them, maybe we would score a 1 for certain elements and a 3 for others, can't really say something about it'*.

Culture and behavior

The next factor which hinders organizations in their growth is described as a main theme: 'culture and behavior'. This main theme is further categorized into three subthemes: change management, purchasing management and supply management. These subthemes are all elements that keep organizations from growing, according to the participating respondents.

According to respondents, change management relates the belief that it is hard to change the behavior of people because they are not careful enough. Respondent #3 for example points out: *'What we want, is to change their behavior. They need to think more carefully. A chain is as strong as the weakest link. People even share their passwords on post its! It seems we can't get that out of their system'*. About the same subtheme, respondent #4 emphasizes that technique is able to solve a lot, but the human factor plays a major role in information security practices: *'Technique can solve a lot of things, but it all starts with the human factor, that's always the weakest link'*. The second subtheme is purchasing management and is about the processes around purchase management. Respondent #7 elaborates on this: *'Often an application or system is almost bought and they realize the information security box must be checked as well. Then it seems as if I'm a very annoying person with all my questions, but they should've involved me from start, that saves time and effort. Security and privacy by design is very important. We are busy with implementing that now at the purchasing department'*. The third subtheme is described as supply management and is more about the contracts and agreements organizations have with their suppliers. About this, respondent #4 points out: *'Supply management is not good enough now, we sign agreements but are not aware of what we do after'*.

Accountant

The last main theme is described as 'accountant' and consists of one subtheme which is described as 'role of IT auditor'. Some of the participating respondents claim that accountancy organizations can contribute to the development in information security maturity through different manners. For example, respondent #4 expects other things from an IT auditor and argues that accountancy organizations need to get back to their core business and stop with too much usage of (theoretical) frameworks: *'Accountants need to stop with all the theories and stuff, get back to the core business: book keeping! I expect a critical view, no questions of a list, good questions and a strategic partner instead of only a pass or a fail for an audit'*. Respondent #5 for example, is convinced of the effect of IT auditors within their own organization if they are able to help CISO's for example by assisting them to realize their own objectives and goals by getting approval of the board: *'An IT-auditor could help us so much more with getting us what we need through approval of the board'*. Furthermore, several respondents found themselves convinced of a change of the role of an IT auditor. These participants argue that working off a check list, just criticizing and judging an audit with a pass or fail does not help them further. Like respondent #3 wants an IT auditor as a ‘strategic partner’, respondent #7 pointed out: *‘An IT-auditor must help and give advice instead of just criticize and judge. Maybe with some sort of growth model’*. Respondent #6 also pointed out that this critical attitude of IT auditors sometimes appears as hostile while noting: ‘*We serve the same purpose, we are no enemies, they could help us with translation’*.

However, there were also other participants who found themselves aware of the conflicting roles of accountancy organizations, respondent #3 elaborated: *‘I don’t think IT auditors are the designated persons to help with this, that means they need to check through an audit, give advice and check if you listened to their advice. I think that’s conflicting, there were several scandals with accountancy firms in the past, I’m afraid the same would happen with this’*.

Table 5: analysis of interviews with respondents from Dutch Public Organizations

Category	**Description**	**Example**
Priorities	Focus is on the many processes and tasks	*'As municipalities we have many tasks and responsibilities, so many processes, information security is often forgotten about and they don't feel the urge to handle this topic'*
	Newness of related tasks and procedures	*'Governance needs to be implemented, but municipalities never did something like this, why would they do it now? It's hard to get these things executed because it's not their priority'*
Time	Rules and regulations with regards to decision making	*'As a municipality we are bound to so many rules before we can decide about something. If a profit organization needs a new employee for a certain department or task, he could be sitting there tomorrow'*
Capacity	Capacity in staff	*'We can't evaluate because we don't have enough time and people'*
		'We simply don't have the people for it'
		'We want to expand the team because we need more capacity to keep things safe, to react on incidents, we simply don't have that capacity now'
		'You can have plans and policies and stuff, but if you don't have the right people for the job? The right people to execute the projects. Else, you can put the plans back in the closet again. We are very busy now with searching for a good ISO for example'
	Capacity in time	*'There is simply no time to do such things like evaluation or anything, in municipalities we often work and live by what the day brings us and people are already busy with that'*
		'We have more than 400 applications, if you want to be in control of all of them, you need time'
	Lack of capacity in knowledge and expertise leads to pushing off related tasks	*'Because managers think they don't have enough knowledge about the topic, they think they can just push it away'*
Resources	Ability to attract right resources in staff	*'I wonder if we are even able to attract the right expertise as a municipality, are we able to offer the right people the salary they can earn elsewhere?'*
Awareness	Knowledge because of recent implemented regulations	*'GDPR related stuff is still relatively fresh'*
	Awareness because of previous incidents	*'The Hof van Twente case opened a lot of eyes and made them aware!'*
		'When people hear about other incidents, they become more aware and alert'
	Knowledge because of internal incidents	*'As harsh as it sounds, an incident helps in raising awareness. People can get really upset when they cause something. Fortunately I never heard someone say that it's not a problem'*
		'When they fail for a phishing test, believe me, those people really get the message!'
	Awareness programs	*'Repeating is the strongest message of advertising!'*
		'Every new employee gets a basic training around the topic and we keep them updated through interesting e-learnings'
	Underestimation of risks	*'They don't realize that a risk is still a risk, regardless of the size of it'*
	Awareness by practice	*'By explaining, people understand, you have to make it practical so it becomes recognizable. People need to know you as well, so they know why and for what they are doing something. That's how you raise awareness and motivation'*
Responsibility and roles	Lack of feeling of responsibility	*'As a CISO I have my responsibilities, the ISO has responsibilities, but the line managers need to know their responsibilities as well'*
		'As a CISO I need to have a controlling and advising role, not an executing one'
		'They need to realize that information security is something for all of us, not only for a CISO'
	Fear of responsibilities	*'They know their role and responsibility, but don't want to have it written down, people don't want to have formal responsibility, they get scared'*
		'When I do a risk analysis, I do that together with the process owner, so that he accepts the risks and the responsibility that comes with that'
	Lack of formalized procedures	*'I think they know what their responsibility is, but we don't have it formalized. Yet! We are busy with formalizing it'*
		'They think that all security related stuff is the responsibility of the CISO'
		'Things are being done for information security, but processes are not yet structured enough, there is no real description for every process'
Frameworks	Lack of fulfilling monitoring frameworks	*'We Plan and Do indeed, but we don't Check and Act after implementation'*
	Usage of ISMS	*'We have it, but do not use it frequently enough yet'*
		'I use ISMS as some sort of PDCA cycle instead of tool. Through ISMS I can Plan, Do and evaluate to Check and Act!'
Knowledge	Knowledge about BIO	*'The BIO is not clear for everybody. I never spoke to operational staff about BIO, only with the board and management'*
		'The BIO is way too technical, I don't want to bother people with that'
Maturity models	Usage of maturity models	*'I know about CMMI, I even included it in our information security policy! But never heard of the other one''*
		'Heard of it, but we don't use it'
	Limited knowledge about maturity models	*'They certainly can help! But not for me, too theoretical'*
		'We don't really use them, but they can be a good guideline'
	Lack of knowledge of maturity models	*'I don't know them that well, heard of it a few times'*
		'No, I haven't heard of them'

	Lack of realization of current levels	*'Because I don't know them and never used them, maybe we would score a 1 for certain elements and a 3 for others, can't really say something about it'*
Culture and behavior	Change management	*'What we want, is to change their behavior. They need to think more carefully. A chain is as strong as the weakest link. People even share their passwords on post its! It seems we can't get that out of their system'*
		'Technique can solve a lot of things, but it all starts with the human factor, that's always the weakest link'
	Purchasing management	*'Often an application or system is almost bought and they realize the information security box must be checked as well. Then it seems as if I'm a very annoying person with all my questions, but they should've involved me from start, that saves time and effort. Security and privacy by design is very important. We are busy with implementing that now at the purchasing 51department'*
	Supply management	*'What I told you, we need to know what we have in store. That's a real change in our culture and way of working'*
		'Supply management is not good enough now, we sign agreements but are not aware of what we do after'
Accountant	Role of IT auditor	*'An IT-auditor must help and give advice instead of just criticize and judge. Maybe with some sort of growth model'*
		'An IT-auditor could help us so much more with getting us what we need through approval of the board'
		'Accountants need to stop with all the theories and stuff, get back to the core business: book keeping! I expect a critical view, no questions of a list, good questions and a strategic partner instead of only a pass or a fail for an audit'
		'We serve the same purpose, we are no enemies, they could help us with translation'
		'I don't think IT auditors are the designated persons to help with this, that means they need to check through an audit, give advice and check if you listened to their advice. I think that's conflicting, there were several scandals with accountancy firms in the past, I'm afraid the same would happen with this'

All of the factors, explained as main themes, subthemes and the citations shown above in Table 4 and Table 5 are considered the most important observed factors during this research, that hinder Dutch Public Organizations to further grow in maturity around information security practices. Moreover, it is visible that a lot of the main themes in both tables match. Therefore it can be concluded that the view of the accountancy organization largely corresponds with the view of experts from the Dutch Public Organizations on this topic. However, in Table 4 there are seven main themes described, whereas Table 5 describes four more, meaning there are in total eleven main themes. Table 4 shows the view of the accountancy organization on the topic of research, this results in a more observing perspective. Thus, this also translates in a difference in amount of subthemes. Whereas Table 4 contains 17 subthemes, Table 5 consists of 27 subthemes. Therefore it can be concluded that Table 5 provides more factors and more in depth information about the current situation at the participating Dutch Public Organizations. Moreover, observing both tables from a more general perspective, from the main themes categorized in Table 4, six out of seven have also been categorized and mentioned in Table 5. The main theme missing from corresponding with all main themes is the main theme of consequences. This main theme is not mentioned in Table 5 nor mentioned during the collection of data during interviews with participating respondents from the Dutch Public Organizations. Furthermore, as concluded, since there are more subthemes categorized in Table 5, it can be seen that this table goes more into depth through the subthemes mentioned. The main theme of priorities which is categorized in both tables contains three subthemes in Table 4, while Table 5 consists of two subthemes. However, two out of three subthemes correspond with one another, despite being formulated in a different way. The third subtheme which is mentioned in Table 4 is related to financial budget priorities. This could be explained as the opinion from an outsider, in this case an IT auditor, which experiences that Dutch Public Organizations, municipalities specifically, have hardship in setting priorities due to financial reasons and the way organizations spend their money. Furthermore, Table 5 compared to Table 4 also consists of the main theme of 'Time' whereas Table 4 does not include this main theme. The reason for mentioning this main theme by the respondents of Table 5 could have to do with the inside information and knowledge about procedures and processes around decision making have, elements that respondents of Table 4 are not aware of. Moreover, the respondents of Table 5 also mention the main theme of 'Capacity' compared to the respondents of Table 4 who did not mention these factors among this main theme. The respondents of Table 5 blame the lack of growth in maturity in information security among others, to the lack of capacity in broad term. While the respondents in Table 4 place these alike factors more among the main theme of 'knowledge and expertise'. In Table 4 it can be seen that the main theme of knowledge and expertise contains of subthemes that are related to proper qualifications, lack of knowledge among employees and lack of knowledge of BIO. As an example, the subtheme related to the lack of knowledge about the BIO is placed into another main theme in Table 5 which is 'knowledge' and is exclusively dedicated to element related to the BIO. Additionally, in comparison to the first table, Table 5 provides the additional main theme of 'resources' whereas Table 4 does not mention this main theme. Next, the main theme of 'awareness' is present in both tables. However, described and further categorized in different subthemes. The difference in the further description of subthemes is expressed in the way Table 4 has a focus on what the accountancy organization experiences in how Dutch Public Organizations react on pressure that derives from external incidents. On the other hand, Table 5 differs within this main theme mostly in subthemes about what organizations do to raise awareness and in how people underestimate the risks that come along this topic of research. Moreover, the main theme of 'frameworks' correspondents to a certain extent, although Table 4 describes one subtheme while Table 5 describes two subthemes. In both tables it is shown that there is a lack of fulfillment of frameworks that ensure monitoring and evaluation of implementation of information security measurements. Nevertheless, Table 5 describes an extra subtheme that is focused on the use of ISMS as a type of framework while this element is not mentioned in Table 4. A reason for this formation of subthemes could be due to the perception of usage of an ISMS, where the participants in Table 4 do not consider an ISMS a tool for monitoring and evaluation while the participants in Table 5 use it in such way. Furthermore, Table 4 describes the main theme of 'consequences' with two different subthemes, while this main theme is not present in Table 5. This could be explained by the view of the type of respondent on this subject. Where the respondents in Table 4 consider this focus of research from a perspective of an accountancy organization and therefore perhaps from a more law abiding perspective. The respondents in Table 4 argue that there are no real consequences for organizations and this could be helpful in growth in maturity. Moreover, the accountancy perspective could also be more considerate from a more business operations perspective in wanting to prevent organizations from political consequences through media. Next, both tables make notice and mention the main theme of 'roles and responsibilities' and have an extensive corresponding between the subthemes within this main theme as well. This demonstrates that both group of respondents have an agreeing view on this factor. Besides, both tables describe about the same subthemes as well despite being formulated in another way. Both tables agree on the importance of formalizing procedures, the danger that comes along the fear of taking responsibilities and the ownership that should be taken by responsible managers or the appointed employees. Furthermore, the results in Table 5 also differ from the results In Table 4 due to the presence of the main theme of 'maturity models' within Table 5. This is mostly due to the set of interview questions that contained questions about this subject for the group of respondents of Table 5 and that were not asked to the group of respondents of Table 4. Moreover, the main theme of 'culture and behavior' is present in both tables while also corresponding in subthemes. Nevertheless, there is one difference: Table 4 describes one extra subtheme as 'risk management' which could be due to perception and interpretation of the respondents on risks. The respondents in Table 4 could view this subject from an accountancy and perhaps more consulting point of view which could lead to growth whereas the respondents from Table 5 place other subthemes among the main theme of culture and behavior.

However, a small note on risks is made in Table 5 but as a subtheme is placed among another main theme, but is indeed mentioned. This means that the view of both group of respondents match on this subject. At last, Table 5 differs from Table 4 through the notation of the main theme of ‘accountant’. This is mostly due to the fact that the group of respondents in Table 5 were asked about their view on the accountancy organization and what could be improved, while this was not asked to the group of respondents in Table 4. Furthermore, These factors can also be linked to the BMIS as presented in Figure 2 which will be done in the next chapter. Moreover, the next chapter goes more into depth on how to handle the mentioned factors and overcome these obstacles to further grow in maturity in information security levels.

5. Conclusion and discussion

This chapter of research provides key findings and the most essential and significant results of this research. Secondly, this chapter defines recommendations for Company X (and other organizations in general) and lists the limitations of this research. Additionally, this chapter suggests further recommendations for future research possibilities.

5.1 Key findings

The aim of this research was to explore the main research question: *"Why are Dutch Public Organizations failing to get their information security on sufficient maturity levels and what could they do in their approach to information security practices to increase these levels?"*. To answer this central research question, literature was analysed to gather knowledge about information security in a general context, what maturity models are available in existing literature and interviews were held with different type of respondents to explore this research question. By doing this, it was found that the view of IT auditors on this topic of research does not deviate that much from what the other group of participating respondents such as CISO's and Team Managers Information gave as their view on this topic. However, this does not mean that both group of respondents gave the same answers and same reasons in factors which hinder Dutch Public Organizations to grow. Thus, the in-depth interviews with the participating respondents from Dutch Public Organizations can be seen as an extension of the factors which play a role. Before the fulfilment of this research there was a gap in the literature with regards to factors that inhibit and hinder these type of organizations in their growth to higher maturity levels. Moreover, it can be concluded that the proposed NBA maturity model does not offer the expected added value among the participating organizations since maturity models in general were not very known. Therefore it was hard for the participating respondents to estimate which maturity level was achieved until now. However, most of the respondents attempted to estimate after explanation of the maturity models and it can be concluded that the participating Dutch Public Organizations fall between level 2 and 3, but also admitting that maybe some elements within the organizations are maybe even on level 1. This indeed does indicate that there is an important need for further growth in this field of research. Among the factors that almost all participating organizations do that help and can increase the growth of these organizations is the programs they propose for increasement of awareness. All organizations consciously act upon this topic of information security by preparing onboardings for new employees, but also by several e-learning programs during this Covid-19 period. Moreover, almost all participating organizations declared they have had intentions of organizing more events for raising awareness for this topic. As factors that inhibit growth in maturity levels, multiple subjects, factors and elements were mentioned by the participating respondents. Nevertheless, it can be concluded that one of the most frequented mentioned factors had to do with the lack of formalization of processes which includes that there is no process owner, meaning that all actions for implementation and compliance regarding information security still need to be initiated by CISO's because there is no ownership and responsibility by appointed (line)managers. There is some sort of fear for this formalization according to respondents. Moreover, participating respondents also claim that due to all the responsibilities and other tasks, the huge amount of applications, there is simply no capacity, to keep busy with information security related practices, in form of employees, knowledge and expertise and time. Therefore, organizations struggle with setting the right priorities and information security comes bottom of the list. Additionally, another frequently mentioned factor is the formalization in processes with regards to monitoring and evaluation of implemented measures. As participants explained, there is no final fulfilment of a PDCA cycle or likewise, since there is Planned and Done, but no Check and subsequent Act on this. It can be stated that organizations are not 'in control' towards this topic of research. Finally, there is deviation among respondents with regards to the role of the IT auditor. However, almost all participants agreed on the fact that they want IT auditors to adopt to a more consulting and advising role instead of the audits they execute with the subsequent result that comes along. Additionally, when looking at the BMIS as presented in the literature in Figure 2, it is still hard to conclude around which dot or interconnection the main reason lies for not growing further in maturity levels. The different factors that are observed and mentioned through data that is gathered could be categorized under multiple dots within the model. There Is no clear dot or interconnection that stands out in covering all the gathered data or one dot or interconnection that significantly needs most attention. It can be stated that the organization as a whole needs improvement, people need to change, processes need further development as well as technology. Therefore it can be concluded that there is no unanimous specific element within the model that needs to be further developed but rather all four dots and six interconnections need improvement in general.

5.2 Recommendations

Among these factors that inhibit Dutch Public Organizations to grow in maturity levels, recommendations can be developed in order to recommend the organizations to turn these factors and handle these elements in order to help and enable them to grow further in maturity with regards to information security practices.

Recommendations for Dutch Public Organizations

One of the factors that was mentioned frequently during this research, was the lack of evaluation and monitoring of implemented measures and the knowledge of maturity models. A recommendation for these firms would be the use of maturity models in policy development regarding information security in the first place. For the reason that maturity models can be used as a guide for process improvement. Therefore maturity models can be a substitute of a Plan Do Check Act cycle. Another factor that was frequently mentioned was the struggle around the setting of the right priorities around the multiple tasks and responsibilities that municipalities have. Because of these multiple tasks and responsibilities, management struggles with information security measurements which results in the sinking of information security related tasks and responsibilities on the priority list. Moreover, another mentioned factor was the lack of formalized processes around information security practices. This can be due to various reasons, one of them could be the lack of ability to prioritize information security matters, another reason could be the lack of time or lack of ownership around information security practices. Moreover, the lack of usage of frameworks and models in policy development can also be counted to the list of reasons why there is lack of formalization of processes. Models that are specifically focused on information security and for example only with a strong focus towards IT related departments, will not be able to attract the attention or increase awareness among other employees or departments. It could be helpful to make use of organization wide models. Therefore it is important to make more use of models in policies around this topic within organizations. Something that could be of recommendation is the use of an information security governance framework as proposed through research by Veiga and Eloff (2007) which Is attached in Appendix IV. This framework offers a guideline to implement information security governance over the whole organization. The framework offers three perspectives: strategical, managerial & operational and technical, it even focuses on employees and the direction of their behavior combined with change management. Meaning this framework can be of help for the further compliancy in information security over the whole organization. Yet, despite offering a framework for an organization wide perspective for compliance in information security, there are mentioned factors which can be overcome through different methods as well which could have a more short term effect. These methods are further described below and categorized in Table 6: Overview of possible methods to overcome factors. First of all, the respondents claim that they experience hardship in setting priorities due to the many responsibilities that Dutch Public Organizations such as municipalities have. This could be overcome by implementing a method organization wide, a priority matrix for example. Such matrix can help prioritize projects and goals, regardless the tasks. Moreover, it helps prioritizing the responsibilities and therefore the tasks that come along with these responsibilities. Such matrix could for example be divided into urgent and non-urgent matters and important and non-important matters. This can help by setting the right goals, attaching a period term can make this more concrete and gain focus as well. The factor of time relates to the amount of time municipalities need before decision can be made due to the many rules and regulations that these type of organizations are bound to. Respondents provided an example about the procedure around hiring staff but this factor also affects decision making around purchasing management. This could be overcome by the implementation of a more effective procedure around decision making. This could be done through the use of a specific system or application that needs to be implemented that makes use of checklists and involves all people or departments that are concerned with the certain topic and through this way certain ‘task groups’ are created to be more effective in their work to save more time around decision making. The factor of capacity was related to the capacity in staff, time and knowledge. This could be overcome to broaden capacity by hiring more expertise within municipalities or to even make current interested employees broaden their own knowledge through courses or new studies to create own experts that are located internally. By attracting or creating new suitable people, the time element diminishes as well. The next factor of resources can be linked to the former factor of capacity because respondents identified their doubt about being able to attract the right people (links to capacity in staff) due to working conditions like salary. The impact that this factor has, could be conquered through different possible ways. One of these for example, is to increase the salary limit within Dutch Public Organizations to be able to somehow be competitive with profit organizations in attracting the right people. This could be justified through making visible that there is shortage of qualified people for jobs around information security practices. Moreover, Dutch Public Organizations could maybe have an image of being old fashioned within working environments and conditions, new promotion campaigns could help prevent this image. Carefully selected and created campaigns by external agencies that are specialized in these subjects to promote working for Dutch Public Organizations. Next, the factor of awareness that needs to help increase information security maturity can be developed through the offering of training and courses. These trainings and courses need to be focused on raising awareness for information security practices. This could be done through multiple ways, one of these is gamification for example. Since it is more important to offer a fun and interactive way of involving employees around these matters. Furthermore, phishing tests throughout the year can help to retain the focus on this subject and by additionally sharing results, people become more aware and learn from this as well. Handing out certificates or awards among these learning processes could also be of help. However, it starts with measuring the current awareness to set goals and clear targets and work upon these. Moreover, the Information Security Governance Framework can offer a wider improvement within this factor as well through a user security management perspective with a focus on user awareness and education and training. The next factor or responsibility and roles which needs to be further improved starts with the basis in formalization of procedures around information security related topics within the organizations. Most of the respondents argued that there is lack of formalized procedures around these topics and people are not willing to take responsibility. In the first place, this needs to be overcome by formalizing procedures through the appointment of product managers or product owners. This could be a first step in order to finalize these procedures and create a feeling of responsibility that is written down which urges and forces these appointed people to further work on this. By attaching consequences (through periodical evaluation assessments for example) for these product owners, they become forced in some way to handle their responsibilities and the rest of their teams. Furthermore, this is one of the factors that can be overcome by implementation of the Information Security Governance Framework since this offers procedures and policies from a managerial and operational perspective in a security policy type of view. The next factor relates to the lack of evaluation and monitoring of measures and is categorized under the factor of frameworks. It is recommended to make use of a single method across the organizations to further implement monitoring and evaluation of implementations around information security practices. A relatively simple method and easy to use is the well-known PDCA cycle that covers plan, do, check and act. However, it is of more importance to implement this with a periodical commitment such as quarterly execution that is written down in the formalized procedures around information security. Moreover, the already recommended Information Security Governance Framework can also be of help around this factor through the measurement element from a strategic and leadership and governance perspective within the framework. Also, the factor of knowledge around the topic was categorized and noted as an important element in not being able to grow in maturity. This relates to the lack knowledge in a general way about information security matters and could be overcome by offering courses as well. Within this factor, courses need to have a more specific focus on the general knowledge related to information security or perhaps the BIO to increase knowledge and awareness at the same time among employees which may probably result in a higher maturity in the long run. These trainings and courses can be performed by experts within the field of information security or cyber security. Additionally, the Information Security Governance Framework can also function as a proper method to increase the knowledge of people. The framework offers an education and training element from a user security management perspective. Another categorized factor is described as the main theme of maturity models which relates to the lack of usage and knowledge of maturity models which automatically translates into a lack of realization of maturity levels. It is of importance, to include a suitable maturity model such as the NBA maturity model or one of the other described security focused maturity models, in policy development. This results in more knowledge and realization of the current situation and therefore the sense of topics that need further improvement and focus. Implementation of maturity model in policy development within Dutch Public Organizations is coherent with the implementation of a PDCA framework to make optimal use of the selected maturity model. By implementation of maturity models, organizations become aware of where they stand in maturity and by usage of evaluation methods every six months or even quarterly, it becomes more clear what organizations need to work on. Another factor which is mentioned in having a role in disabling further growth is culture and behavior within Dutch Public Organizations. This relates to purchase and supply management among other things. Respondents argue that purchasing processes are not fully optimized since information security related topics around purchasing are often forgotten about and are thought about at the last stages. To overcome this, a helpful tool needs to be implemented that has a firm focus on task management. Through the help of a checklist that counts every concerned department, the tool ensures that everybody is involved from the start to make sure that nothing is forgotten about or need to be handled at the last stages. Moreover, an evaluation tool can also be helpful with regards to supply management. It is recommended to make use of a tool that helps to inventorize the different suppliers of the organization on a periodical basis. This needs to include elements for example like contract management and SLA management to be able to carefully select the suppliers that need further development on these grounds. Moreover, the Information Security Governance Framework can provide help in improving risk management as well. At last, respondents also argued that the role of the accountant needs further improvement. This could be executed through more frequent visits or meetings to assist the organizations and automatically develop to a more consulting role. By only visiting or auditing the organizations on basis of an the interim- and end year audit, the consultant stays stuck in his role of auditor instead of consultant. These meetings need to have a more in-depth character or can be even fulfilled through working on location on a quarterly basis for example. This ensures a better connection and feeling with the organization to be able to provide advices and therefore help organizations to a higher maturity.

Table 6: Overview of possible methods to overcome factors

Main theme/factor	Possible method to overcome
Priorities	- Implementation of priority matrix across organization
Time	- Implementation of systems or applications to be more time effective through checklists in the form of applications or systems
Capacity	- Create opportunities for current employees to study for new related roles
Resources	- New promotion campaigns with a focus on attracting people for jobs within Dutch Public Organizations - Increase salary limit
Awareness	- Offering awareness trainings and courses - Information Security Governance Framework
Responsibility and roles	- Specifically designed procedures around information security - Information Security Governance Framework
Frameworks	- Standardized method across organization to ensure evaluation - Information Security Governance Framework
Knowledge	- Offering of courses or hiring of experts to train employees - Information Security Governance Framework
Maturity models	- Integration of maturity models in policy development in combination with evaluation frameworks
Culture and behavior	- Implementation of tools to involve every concerned department - Information Security Governance Framework
Accountant	- Frequent visits and working on premise to grow to a more consulting role.

Recommendations for Company X

As mentioned, a recommendation for Company X would be to build up to a more consulting role, where an IT Advisory department can have a consulting role instead of a controlling one. This could improve the growth of maturity levels of Dutch Public Organizations in the field. Some of the mentioned comments that came up during the interviews with the participating respondents had to do with the results that municipalities now had to hear if they passed or failed an audit but rather receive more hands-on advice. CISO's at municipalities rather hear about what they can do their selves with the help of an IT auditor. Participating respondents now mention that a critical attitude is not a problem, but rather hear what needs to be done. Instead of just a checklist with a pass or fail as a result, CISO's rather hear what needs to be done to further grow. Another specific respondent also claimed that an IT auditor would be of great help if the management letter was translated into an advice that could be presented to the board of a municipality to help with realizing the intended objectives of the security team. Something that Company X could be of help in this, is to establish an own maturity model that could be used for their own clients with hands-on advice in what to do to reach higher levels. Being able to develop such model could be of benefit for Company X's own clients. However, something that needs to be kept in mind is that this could lead to the conflicting role of the accountancy firm in general, the acceptance of the role of advisor and controller at the same time. Another case that an accountancy firm as Company X could do and improve, is to provide more hands-on training methods to increase awareness in the first place. This could result into higher engagement from an employee perspective at Dutch Public Organizations around the topic of information security. Moreover, specific actions like these can also lead more to the demanded role that is asked from an IT auditor at an accountancy firm. Finally, it is important for Company X to assess clients on an organization wide basis with a focus on information security practices together with the responsible CISO for example within the organization. This could be helpful in prioritizing the most important elements that need most improvement and development.

5.3 Limitations and future research

Nevertheless, it is important to take note of certain limitations within this study as well. First of all, data from Dutch Public Organizations was exclusively gathered from organizations in form of municipalities. Additionally, this data was gathered, from relatively big municipalities with at least 50.000 inhabitants and at least 400 employees and not from smaller organizations. This means that conclusions are perhaps not relevant for these smaller organizations. Moreover, due to COVID-19 restrictions all interviews needed to be held, which means that interviews needed to be transcribed, however, some of these interviews contained weird noises due to a bad internet connection. Moreover, due to a lack time, the researcher was not able to find more respondents in the form of more persons within the same organizations to gain more insights from other perspectives. Or perhaps even in the form of more municipalities or other sorts of Dutch Public Organizations. At last, within this research there was no usage of quantitative data collection through surveys for example. Something which along the process of this research could have been useful as well, to gather more insight in the most important topics within this field of research.

However, among these limitations also certain suggestions for future research must be considered. While there is belief that the extent of this research is capable of providing solid results and recommendations, there still remains potential of further extension of research in this broad field. Since the focus of this research was specifically on Dutch Public Organizations, and more specifically municipalities that acted as respondents, it cannot be proven that the results of this study are applicable on every type of public organizations. It even cannot be proven that the results of this research are applicable on other municipalities in an international context. Additionally, this also means that results of research are not directly applicable on private organizations. Thus it is advised to further broaden this research, applied on other sorts of organizations, in different contexts, different segments, other institutions or even in different countries in international contexts. Yet, this research has developed a basis that can be used to further explore other topics within this field of research.

References

Anderson, R. (2007). Thematic content analysis (TCA). *Descriptive presentation of qualitative data*, 1-4.

Ashenden, D. (2008). Information Security management: A human challenge? *nformation security technical report, 13(4)*, 195-201. DOI:10.1016/j.istr.2008.10.006

Becker, J. K. (2009). Developing maturity models for IT management. *Business & Information Systems Engineering, 1(3)*, 213-222. DOI: 10.1007/s12599-009-0044-5

Bio-overheid. (2020). BIO versie 1 .

Bligh-Wall, S. (2017). Industry 4.0: Security imperatives for IoT—converging networks, increasing risks. *Cyber security: a peer-reviewed journal, 1(1)*, 61-68.

Bloor, M. &. (2006). Theoretical saturation. *Keywords in qualitative methods*, 156-166.

Boeije, H. (2009). Analysis in qualitative research. In H. Boeije, *Analysis in qualitative research.* London: Sage Publications.

Boss, S. R. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18(2)*, 151-164. DOI: 10.1057/ejis.2009

Bryman, A. (2016). Social research methods. . In A. Bryman, *Social research methods. .* Oxford: Oxford university press.

Cooke-Davies, T. (2004). Project management maturity models. *The Wiley guide to managing projects*, 1234-1255. DOI: 10.1002/9780470172391

Creswell, J. W. (2016). Qualitative inquiry and research design: Choosing among five approaches. In *Qualitative inquiry and research design: Choosing among five approaches.* Sage publications.

De Gelderlander. (2021, November 17). *DeGelderlander.nl*. Retrieved from www.degelderlander.nl: https://www.gelderlander.nl/ede/hackers-achterhalen-inloggegevens-edese-ambtenaar-en-versturen-grote-hoeveelheden-phishingmails~ab857a0c/?referrer=https%3A%2F%2Fwww.linkedin.com%2F&referrer=https%3A%2F%2Fmyprivacy.dpgmedia.nl%2Fconsent%3FsiteKey%3DOom2kBL

De Haes, S. &. (2004). IT governance and its mechanisms. *Information systems control journal, 1*, 27-33.

De Lange, J. V. (2015). Better information security management in municipalities. *IEEE.*, 1-10.

De Stentor. (2019, June). *DeStentor.nl*. Retrieved from www.DeStentor.nl: https://www.destentor.nl/achterhoek/gemeente-lochem-na-hack-weer-bereikbaar~ab536f4a/

Digitale Overheid. (2021, December 18). *Digitaleoverheid.nl*. Retrieved from www.digitaleoverheid.nl: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/informatieveiligheid/kaders-voor-informatieveiligheid/baseline-informatiebeveiliging-overheid/

Duane, A. M. (2012). A conceptual stages of growth model for managing an organization's social media business profile. *SMBP*.
DOI: 10.1515/ijm-2017-0015

Dzazali, S. S. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. *Government Information Quarterly, 26(4)*, 584-593.
DOI: 10.1016/j.giq.2009.04.004

IBD. (2020). *Jaaroverzicht 2019.* Den Haag: Informatiebeveiligingsdienst.

IBD. (2021). *AVG Borgingsproduct 2.0.* Den Haag: Informatie Beveiligings Dienst.

IBD. (2021). *Jaaroverzicht 2020.* Den Haag: Informatiebeveiligingsdienst.

International Telecommunications Union (ITU). . (2008). TU-TX.1205:series X: data networks, open system communications andsecurity: telecommunication security: overview ofcybersecurity 2008.

ISO/IEC. (n.d.). *Information technology — Security techniques — Information security management systems — Requirements.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en.

Johnson, J. L. (2014). A comparison of international information security regulations. *Interdisciplinary Journal of Information, Knowledge, and Management, 9*, 89-116.
DOI: 10.28945/1963

Kaur, J. &. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. *2013 International Conference on*

Research and Innovation in Information Systems (ICRIIS), 286-290. DOI: 10.1109/ICRIIS.2013.6716723

Khando, K. G. (2021). Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review. *Computers & Security*. DOI: 10.1016/j.cose.2021.102267

Khoshgoftar, M. &. (2009). "Comparison of maturity models.". *IEEE International Conference on Computer Science and Information Technology*, 297-301. DOI: 10.1109/ICCSIT.2009.5234402

Kiely, L. &. (2006). Systemic security management. *IEEE security & privacy, 4(6)*, 74-77. DOI: 10.1109/MSP.2006.167

King, J. L. (1984). Evolution and organizational information systems: an assessment of Nolan's stage model. *Communications of the ACM, 27(5)*, 466-475. DOI: 10.1145/358189.358074

Klimko, G. (2001). Knowledge management and maturity models: Building common understanding. In G. Klimko, *Knowledge management and maturity models: Building common understanding.* (pp. 269-278). Bled, Slovenia. DOI: 10.1590/0104-530X3890-19

Kohlegger, M. M. (2009). Understanding maturity models. Results of a structured content analysis. 51-61.

Koninklijke Nederlandse Beroepsorganisatie van Accountants. (2021, december 10). *nba.nl*. Retrieved from NBA: https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/

Le, N. T. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing.* DOI: 10.12694/scpe.v18i4.1329

Malecki, F. (2020). Overcoming the security risks of remote working. *Computer Fraud & Security, 2020(7)*, 10-12. DOI: 10.1016/S1361-3723(20)30074-9

Moormann, J. &. (2006). IT in der Finanzbranche: Management und Methoden. In J. &. Moormann, *IT in der Finanzbranche: Management und Methoden.* Heidelberg: Springer Science & Business Media.

NOS. (2021, March 16). *NOS*. Retrieved from NOS.nl: https://nos.nl/artikel/2372868-hack-bij-gemeente-hof-van-twente-veroorzaakt-door-te-simpel-wachtwoord

Paulk, M. C. (1993). Capability maturity model, version 1.1. *IEEE Software, 10(4)*, 18-27. DOI: 10.1109/52.219617

Pilorget, L. &. (2018). IT Management. In L. &. Pilorget, *IT Management.* Wiesbaden: Springer.
DOI: 10.13140/RG.2.2.19837.18405

Roessing, R. V. (2010). The ISACA business model for information security: An integrative and innovative approach. *ISSE 2009 Securing Electronic Business Processes* , 37-47.
DOI: 10.1007/978-3-8348-9363-5_4

Saleh, M. F. (2011). Information security maturity model. *International Journal of Computer Science and Security (IJCSS), 5(3)*, 21.

Schneier, B. (2015). Secrets and lies: digital security in a networked world.

Somers, E. (2021). *Cyber security in the public sector: The implementation of the BIO.* Tilburg: Tilburg University.

Srinivas, J. D. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188.
DOI: 10.1016/j.future.2018.09.063

Stoneburner, G. G. (2002). Stoneburner, G., Goguen, A., & Feringa, A. *Nist special publication, 800(30)*, 800-30.

Van Niekerk, J. F. (2010). Information security culture: A management perspective. *Computers & security, 29(4)*, 476-486.
DOI: 10.1016/j.cose.2009.10.005

Veiga, A. D. (2007). An information security governance framework. *Information systems management, 24(4)*, 361-372.
DOI: 10.1145/1655168.1655170

von Roessing, R. (2010). The ISACA Business Model for Information Security: An Integrative and Innovative Approach. In R. von Roessing, *The ISACA Business Model for Information Security: An Integrative and Innovative Approach.* (pp. 37-47). Vieweg+ Teubner.

Von Solms, R. &. (2013). From information security to cyber security. *Computers & Security 38*, 97-102. DOI: 10.1016/j.cose.2013.04.004

Weill, P. &. (2004). IT governance: How top performers manage IT decision rights for superior results. In P. &. Weill, *IT governance: How top performers manage IT decision rights for superior results.* Harvard Business Press.

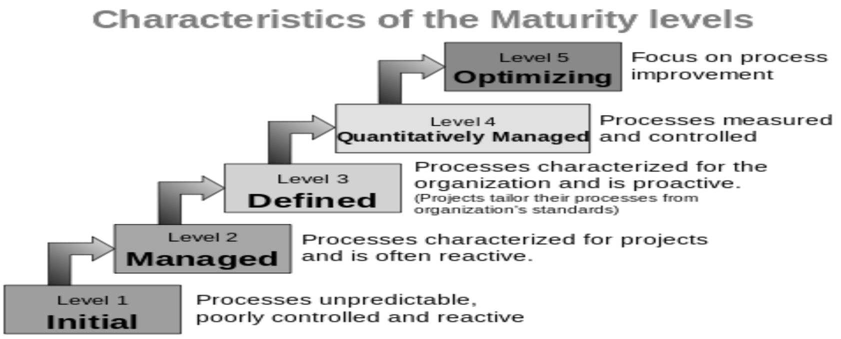
Weill, P. &. (2005). How effective is your IT governance. *Centre for Information Systems Research, Research Briefing, 5.*

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. . *Information and software technology*, 1317-1339. DOI: 10.1016/j.infsof.2012.07.007

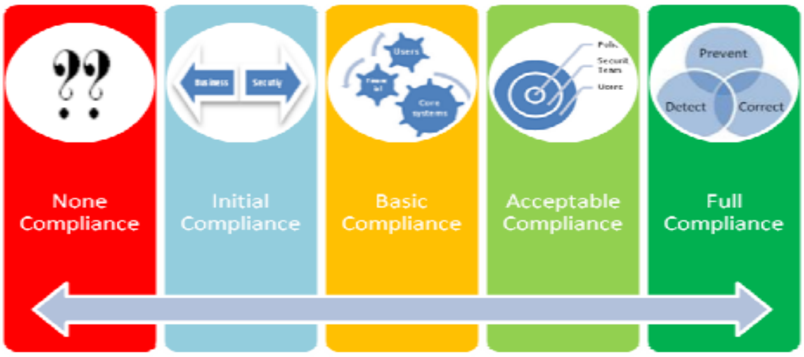
Whitman, M. E. (2009). Principles of information security. In M. E. Whitman, *Principles of information security.* Boston: Cengage learning.

Appendix I: Maturity models

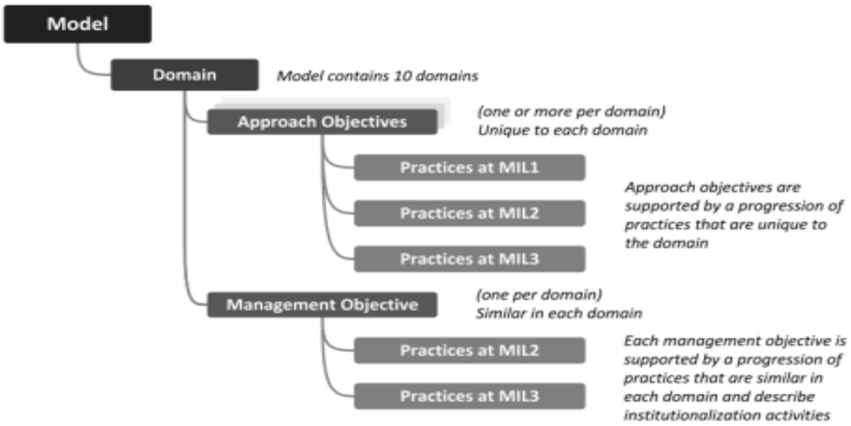
- CMMI IN LOPENDE TEKST EVT.


Characteristics of the Maturity levels
Level 5 Optimizing
Focus on process improvement
Level 4 Quantitatively Managed
Processes measured and controlled
Level 3 Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2 Managed
Processes characterized for projects and is often reactive.
Level 1 Initial
Processes unpredictable, poorly controlled and reactive

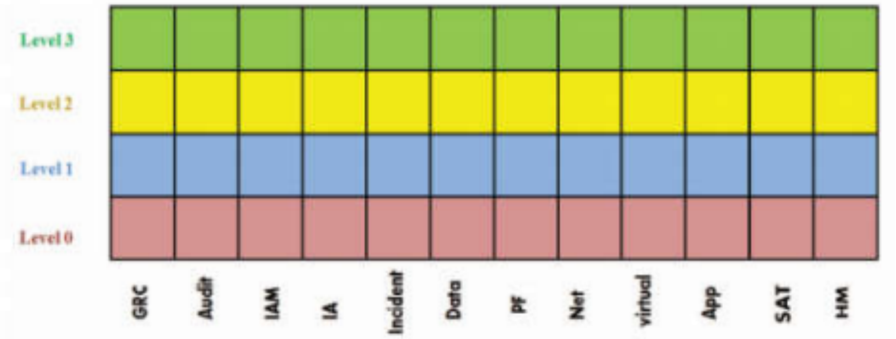
- ISMM



- C2M2


Model
Domain
Model contains 10 domains
Approach Objectives
(one or more per domain)
Unique to each domain
Practices at MIL1
Practices at MIL2
Practices at MIL3
Approach objectives are supported by a progression of practices that are unique to the domain
Management Objective
(one per domain)
Similar in each domain
Practices at MIL2
Practices at MIL3
Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities

- CMMCCS



Appendix II: Interview questionnaire I

Interview questions for Company X's IT auditors and advisors

- Wie ben je? | *Who are you?*
- Wat is jouw rol binnen Company X? | *What is your role at Company X?*
- Wat zijn je verantwoordelijkheden? | *What are your responsibilities?*
- Waar bestaat jouw portefeuille grotendeels uit? | *What does your portfolio mostly consist of in terms of type of organizations?*
- Wat is jouw ervaring met informatiebeveiliging bij gemeentes? | *What is your experience with information security within municipalities?*
- In hoeverre denk jij, dat klanten op de hoogte zijn van maatregelen omtrent informatiebeveiliging? | *To what extent do you think that organizations are aware of measures regarding information security?*
- In hoeverre denk jij, dat klanten (buiten CISO's/ISO's om) op de hoogte zijn van maatregelen als de BIO? | *To what extent, do you think that organizations, except CISO's, are aware about measures like BIO?*
- Hoe denk jij zelf over de BIO? | *What is your own opinion about BIO?*
- Waar ervaren klanten volgens jou het meest problemen? Welke factoren denk je dan aan? (praktische/concrete voorbeelden) | *Where are organizations experiencing most issues? Which factors are you thinking about?*
- Waar hebben klanten volgens jou het meest moeite mee bij implementatie van een niveau wat voldoende is? | *What are organizations struggling with most, when attempting to implement a level which they consider sufficient?*
- Wat is de belangrijkste reden/valkuil waarom klanten niet naar een hoger niveau gaan? | *What is the most important reason why organizations cannot achieve higher levels?*
- Hoe help jij klanten/organisaties hierbij? | *How do you help organizations with this matter?*
- Is er nog iets wat je kwijt wil over dit onderwerp of over hetgeen wat we hebben besproken? | *Is there something else you want to mention about this subject?*

Appendix III: Interview questionnaire II

Interview questions for Dutch Public Organizations

Vragen ter introductie van respondent | *Introduction questions for respondent*

- Wie bent u? | *Who are you?*
- Wat is uw functie binnen organisatie X? | *What is your role within organization X?*
- Wat zijn binnen uw functie, uw verantwoordelijkheden? | *What are your responsibilities?*
- Hoe lang houdt u zich al bezig met informatiebeveiliging? | *For how long have you been working with information security related topics?*
- Zijn er ooit incidenten geweest met betrekking tot informatiebeveiliging binnen de organisatie? | *Have you ever experienced incidents regarding information security?*

Algemene vragen IB | *General questions information security*

- In hoeverre denkt u dat de informatiebeveiliging binnen uw organisatie op orde is? | *To what extent do you think information security is okay within the organization?*
- Wat gaat volgens u goed en wat kan beter? | *What is going well and what could be improved?*
- Hoe activeert u intrinsieke motivatie van medewerkers nu om bezig te houden met informatiebeveiliging? | *How can you activate intrinsic motivation of employees to get going with information security?*
- Wat is uw ervaring op het gebied van intrinsieke motivatie van medewerkers op informatiebeveiliging. Wat werkt volgens u goed en wat kan beter? | *What is your experience regarding motivation of employees with information security? What works well and what could be improved?*
- In hoeverre is de BIO duidelijk voor medewerkers binnen alle lagen van de organisatie? | *To what extent is the BIO clear for employees (within all hierarchical layers)?*
- In hoeverre is men (directie, managers, medewerkers) betrokken bij implementatie van BIO/informatiebeveiliging maatregelen? | *To what extent are people (within all hierarchical layers) involved in implementation of BIO/information security measures?*
- Hoe kunt u de betrokkenheid omtrent informatiebeveiliging verhogen? | *How can you improve and increase involvement around information security?*
- Zijn medewerkers zich bewust van waar de dingen fout kunnen lopen? | *Are employees aware of what and where things can go wrong?*
- Weten medewerkers welke risico's ze lopen? | *Are employees aware of the risks they are working with?*
- Weten medewerkers waar ze melding moeten maken als ze een beveiligingsincident hebben meegemaakt of ontdekt? | *Do employees know what to do after an incident?*

Rollen en verantwoordelijkheden | *Roles and responsibilities*

- Eigenaarschap tonen, hoe kijkt u daar tegen aan op gebied van informatiebeveiliging? | *What do you experience around ownership regarding information security?*
- In hoeverre zijn rollen en verantwoordelijkheden rond informatiebeveiliging duidelijk verdeeld? | *To what extent are roles and responsibilities around information security clearly distributed?*
- Nemen mensen hun verantwoordelijkheid ook? | *Do people take their responsibility?*

- Wat kan daarin beter? | *What could be improved?*

Frameworks and PDCA

- In hoeverre worden security frameworks meegenomen in beleid omtrent informatiebeveiliging? | *To what extent are security and frameworks considered in policy making?*
- Op welke wijze/methode wordt informatiebeveiliging beheerst? | *By what manner or method do you control information security?*
- Maken jullie gebruik van Information Security Management Systems (ISMS)? | *Do you make use of ISMS?*
- Kijkend naar de 5 steps van cyber security framework: is er aan alle 5 genoeg aandacht besteed? | *Do you pay enough attention to all 5 elements of the 5 steps of cyber security framework?*
- Hoe komen jullie tot verbeterplannen wat betreft informatiebeveiliging? | *How do you propose improvement policy around information security?*
- Hoe houden jullie toezicht op voortgang van verbeteringen? | *How do you monitor improvements?*

Volwassenheid | *Maturity*

- Bent u bekend met volwassenheidsmodellen? Zoals die van het NBA of CMMI?
- Waar denkt u dat de organisatie zich nu zal bevinden? Op het volwassenheidsmodel van het NBA?
- Welk niveau ambieert u, voor de organisatie?
- Bent u tevreden met de groei die uw organisatie doormaakt op gebied van informatiebeveiliging? Zijn er concrete plannen voor groei op korte termijn?
- Kunnen volwassenheidsmodellen bijdragen aan de groei van IB? Voor u als CISO/ISO, maar ook voor de organisatie in het algemeen?

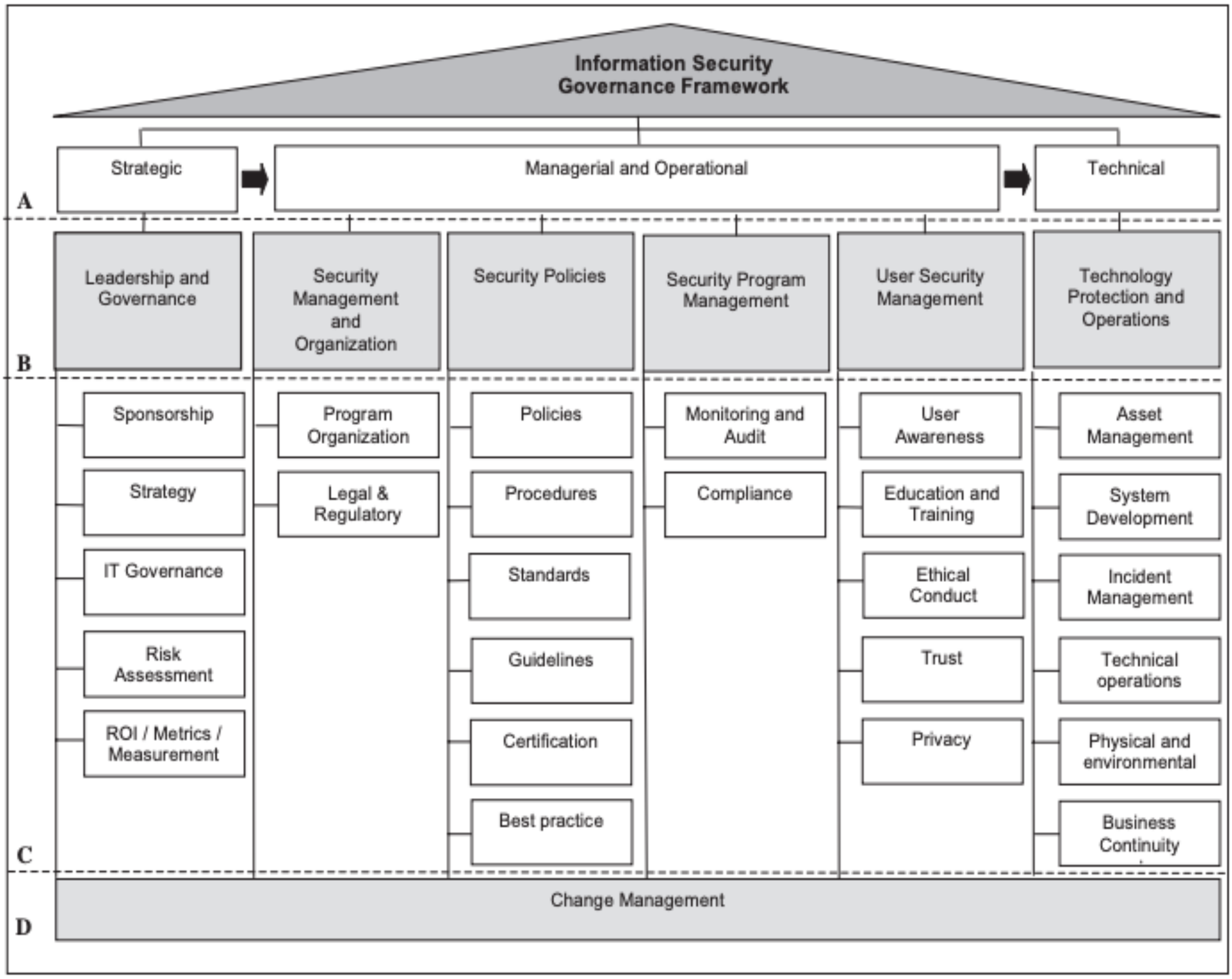
Rol IT-auditor | *Role of IT-auditor*

- Wat verwacht u van een IT-auditor om te helpen bij het groeien van de organisatie op het gebied van informatiebeveiliging? | *What do you expect from an IT-auditor to help by growing in information security?*
- Wat verwacht u van een beveiligingsadviseur/consultant om te helpen op het gebied van informatiebeveiliging? | *What do you expect from an security advisor or consultant to help by growing in information security?*
- Zijn er zaken die IT-auditors en advisors kunnen verbeteren om de organisatie beter te helpen? | *Is there anything that IT-auditors can improve in their job to help your organization in a better way?*

Afsluiting | *Close up*

- Is er nog iets wat je kwijt wil over hetgeen besproken? Dingen die nog niet gezegd zijn? | *Is there anything you want to share besides the things we did not speak about yet?*

Appendix IV: Information Security Governance Framework


Information Security Governance Framework
Strategic
Managerial and Operational
Technical
A
Leadership and Governance
Security Management and Organization
Security Policies
Security Program Management
User Security Management
Technology Protection and Operations
B
Sponsorship
Strategy
IT Governance
Risk Assessment
ROI / Metrics / Measurement
Program Organization
Legal & Regulatory
Policies
Procedures
Standards
Guidelines
Certification
Best practice
Monitoring and Audit
Compliance
User Awareness
Education and Training
Ethical Conduct
Trust
Privacy
Asset Management
System Development
Incident Management
Technical operations
Physical and environmental
Business Continuity
C
Change Management
D