SECURITY BY DECISION-MAKING

A DECISION-MAKING CAPABILITY MODEL FOR SECURITY COUNTERMEASURES

M.S. KORIDON

NORTHWAVE
Intelligent Security Operations

UNIVERSITY OF TWENTE.

UNIVERSITY OF TWENTE.

Business Information Technology

Master Thesis

SECURITY BY DECISION-MAKING:

A Decision-Making Capability Model for Security Countermeasures

M.S. (Matthijs) Koridon

1st Supervisor prof. dr. ir. L.J.M. (Bart) Nieuwenhuis
Faculty of Behavioural Management & Social sciences
Department of Industrial Engineering and Business Information Systems
University of Twente

2nd Supervisor dr. M. (Maya) Daneva
Faculty of Electrical Engineering, Mathematics and Computer Science
Department of Services, Cyber security & Safety
University of Twente

Company supervisor E.R. (Eberly) Haalboom, MSc CISM
Northwave BV

M.S. (Matthijs) Koridon
Student number: 1368524
m.s.koridon@alumnus.utwente.nl

Security by decision-making:
A Decision-Making Capability Model for Security Countermeasures

Master Thesis
Business Information Technology: IT Management & Innovation
July 12, 2019

Supervisors: prof. dr. ir. L.J.M. (Bart) Nieuwenhuis and dr. M. (Maya) Daneva
Company supervisor: E.R. (Eberly) Haalboom, MSc CISM

University of Twente
Business Information Technology
Faculty of Electrical Engineering, Mathematics and Computer Science

Drienerlolaan 5
7522NB Enschede, The Netherlands

Abstract

In organisations, decision-making about choosing the right security countermeasure to mitigate risks is a complex task. In order to aid organisations in establishing a decision-making process that enables them to make the right choice for countermeasures, this research introduces the Decision-Making Capability Model for Security Countermeasures.

Through a systematic literature review of 500 papers, a study of 6 maturity capability models and interviews with 5 security consultants a list with important decision-making factors has been compiled. This list is discussed with 12 decision-makers from practice in a three-round Delphi study. Based on the Delphi study, the Decision-Making Capability Model for Security Countermeasures has been produced. The model consists of 8 factors that should be included in the decision-making process about countermeasures. An example of a found factor is '*Comply to laws, regulations and contracts*'. The combination of factors describe all aspects of the decision-making process about security countermeasures.

To validate the model, two interviews with security consultants and two case studies about the Decision-Making Capability Model for Security Countermeasures been carried out. This has demonstrated the value of the capability model for self-assessment of the decision-making process of the organisation in order to improve the decision-making process. Furthermore, the model presents an accurate view of the capability of the organisation. The model can further be improved by adding an answer in between 'Yes' and 'No' in order to make the results of the model less harsh and more fitted towards organisations. In addition to improving this capability model, research should look into the decision-making process of different organisations to understand them even better. This understanding can lead to an improved fit of the models created in research and the use practice has for them.

The main contribution of this research is a model that can assess and help improve the decision-making process about security countermeasures. Combining academic and practical sources provided a comprehensive view on the decision-making process about countermeasures and the important factors that should be taken into account in this process. Eventually, this process can provide effective security countermeasures and an improved information security of the organisation.

Preface

Nieuwegein, July 5, 2019

Dear reader,

Thank you for your interest in reading my master thesis. This research has been done to complete my master program Business Information Technology at the University of Twente. I have been studying at the University of Twente for several years now, but that time is now coming to an end. The past years I have been developing my personal, academic and professional skills. But now, my '*student life*' will end and a new challenge will be on the way.

I would like to thank people who were important to the development of this thesis. First of all, thanks to my supervisors from the University of Twente, Bart and Maya. During our meetings at the university we always tackled some issues at hand so I could continue with the next important steps. Also Abhishta who was present during most of our meetings provided me with valuable feedback, so thanks! Of course also a big thanks to my supervisor from Northwave, Eberly, who helped me during my research often. Not only Eberly, but the whole Business Security team at Northwave supported me with contributions to the research, valuable input, discussions and the needed diversions with the beloved soundboard. I would furthermore like to thank the interviewees and panellists of the Delphi-study for their time invested in this research. I hope the research provides you with interesting insights.

Furthermore, I would like to thank Martijn for our good discussions on security and of course letting me sleep-over this past period. And, last but not least, I would like to thank my girlfriend, Kyra, and my family for their support these past years and in particular during the development of this thesis.

I wish you pleasant reading.

Kind regards,

Matthijs Koridon

Contents

List of Figures

List of Tables

List of Abbreviations

2FA	Two Factor Authentication
CIA	Confidentiality, integrity, availability
CISO	Chief Information Security Officer
DMCMSC	Decision-Making Capability Model for Security Countermeasures
FIL	Factor Indicator Level
GDPR	General Data Protection Regulation
IS	Information Security
ISMS	Information Security Management System
IT	Information Technology
MCM	Maturity Capability Model
PDCA	Plan, Do, Check, Act-cycle
RM	Risk Management
ROA	Return on Attack
ROI	Return on Investment
ROSI	Return on Security Investment
SLR	Systematic Literature Review
SO	Security Officer

Part I

Background

1 Introduction

> *In the 21st century, we can't create security by building walls.*
>
> **— James G. Stravridis**
> (Admiral of the United Stated Navy)

It is impossible to imagine our world without information technology (IT). Almost all processes and systems of organisations are in some way dependent on IT. This makes information security (IS) essential to prevent from disruptions in business-as-usual. Unfortunately, the news is filled with articles about DDoS-attacks (NOS, 2018), hacking (The Guardian, 2018) and other threats (NCTV, 2019) that do disrupt the daily operations of the targeted organisations. Over the last years IS has become a very important topic to stay in business.

1.1 Background

Information security is the preservation of *confidentiality*, *integrity* and *availability* of information (ISO/IEC, 2018b). Organisations try to keep unauthorised people from accessing and altering information, while the information remains accessible for authorised personnel. In order to do so, organisations worldwide have started to invest massively in IS in the past few years. It is expected that in 2019 the worldwide investment in IS surpasses $124 billion (Gartner, Inc., 2018). This is not surprising, as the total of losses caused by cybercrime is estimated to have risen to more than $600 billion (McAfee, 2018). In the United Kingdom 43% of the organisations have experienced a cyber security breach in 2018 (Department for Digital, Culture, Media and Sport, 2018). Organisations focus more and more on limiting the effect that cybercrime has on them. Nonetheless, the threats to organisations remain large (NCTV, 2019). The question is how the organisation lets threats impact its business.

Risk is the potential of a threat exploiting a vulnerability and thereby causing harm to an organisation (ISO/IEC, 2018b). Often risks are characterised in two dimensions: the chance of occurrence and the potential loss the risk could cause. In order to coordinate activities to direct and control risks, organisations use risk management (RM) (ISO/IEC, 2018b). The current investments in IS show that organisations are thinking about the risks they face and are trying to reduce these risks. By using RM the organisation tries to stay on top of their risks and keep their business secure.

Naturally, not every penny of the budget can be spend on security. This leads to questions about what to spend the limited budget on. Effective risk management is challenging and this is reflected in current literature. For instance, the academic world has introduced a grand number of different models, metrics and frameworks to aid practice in IS. Unfortunately, there is a gap between practice and literature and scholars ask for more research on how decisions in practice are made and how literature could help the decision-making (Weishäupl et al., 2018). According to Dor and Elovici (2016) there should be a decision support method for security practitioners in order to help accomplish his tasks. This is also concluded by Fenz et al. (2011) and Ekelhart et al. (2009). They state that decision makers have the task to select the most appropriate set of IT security investments from an great spectrum of alternatives. Existing methods for making these decisions provide decision makers with inadequate or little intuitive decision support.

Organisations are left with various questions about how to invest in IS, such as "*Should a firm invest in IT security to achieve a competitive advantage compared to other firms in the industry sector and if so, how much and in what security resource should be invested?*" (Weishäupl et al., 2015b). It could be worth investing in IS to get a competitive advantage, as Chehrehpak et al. (2014) has shown that a well implemented information security management system (ISMS) increases marketing and sales. This view is also shared by a lot of organisations as 89% of business say that improving their cyber security will enhance customer loyalty (Vodafone, 2017). However, what actions should the organisation then take?

Organisations look for ways to best protect vulnerabilities with a limited budget (Panaousis et al., 2014). The question then rises "*How should a firm allocate its security budget to the different technological security resources to gain the highest return?*" (Weishäupl et al., 2015b). Chief Information Security Officers (CISOs) are challenged with these questions and have to answer questions like "*Among our top risks, what's the return on investment for mitigation?*" and "*Would implementing two-factor authentication reduce the probable losses enough to justify the investment?*" on a daily basis (Sana, 2019). These questions are difficult to answer and become more relevant every day. To become more secure, organisations should be able to make justified decisions between alternative measures that can be implemented.

1.2 Research goals

To become more secure as an organisation, the organisation needs to be capable of making the right decisions about which security countermeasure to take to mitigate security risks. Knowing what inputs are needed in order to make the right decision is a vital next step in improving the security decision-making capability of the organisation. This would help to bridge the gap between academic models and methods and the practice, which currently have the tendency to fall back to best practices (Ekelhart et al., 2009). All interview partners in Weishäupl et al. (2018) stated that no standardised decision processes have been established

to determine the optimal amount, time and allocation of investment. Although there are a number of models and methodologies available in literature to determine the size of budget or choose the investment (e.g. Gordon and Loeb, 2002; Cavusoglu et al., 2008) there is a large gap between the proposed model or methodology and the practice. This gap is thought to be there because of the high complexity of the decisions (Weishäupl et al., 2018) and the amount of work it takes to use scientific model. To provide insight in the decision-making process about countermeasures, it is vital to understand what factors contribute to well chosen countermeasures. Therefore, knowing what inputs are of vital importance to decision-making about countermeasures that improve the IS of the organisation, would be a giant step in the right direction.

As a lot of organisations currently are already investing in IS, decision-makers should be enabled to measure the capability of their decision-making process. This would provide them with insight in what factors to make decisions they currently include and which they do not. A capability model supports measuring whether or not an organisation is able to achieve their goals in a specific process area (CMMI Product Team, 2010).

The aim of this research is to improve IS for organisations. In order to improve IS, organisations need to be more capable of choosing the adequate countermeasures to prevent risks from occurring. As no comprehensive or standard decision-making process is currently available in literature or practice, the performance of an organisation's decision-making process is hard to assess. By using a capability model that assesses the inclusion of certain important factors, an indicator of this performance can be given. The goal of this research (see also Figure 1.1) framed in the way of Wieringa (2014) is:

> Improve *security risk management* by *designing a capability model* that *gives a performance indicator of decision-making* in order to *rationally reduce risks to an acceptable level*.

In order to create the capability model, there are a five questions that need to be answered. The main research question to achieve the research goal is as follows:

> **Main research question:** What factors should a capability model include that assesses the decision-making process about security countermeasures?

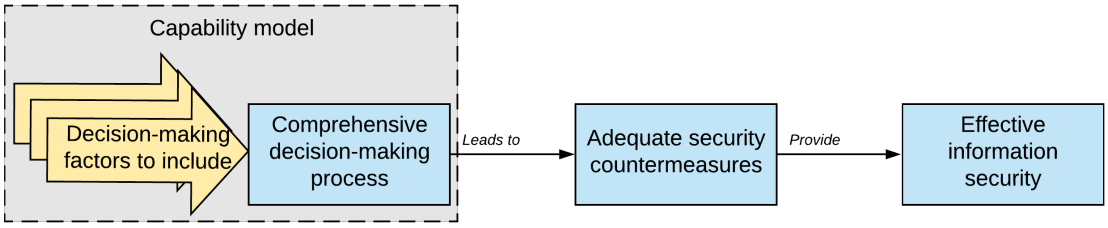


Figure 1.1.: Conceptual model of research in relation to improved information security

To answer the main research question four sub-questions need to be answered. These sub-questions provide two perspectives on the problem: both scientific and practical.

SQ1 What does the overall process of risk management look like and where does the process of deciding about security countermeasures fit in?

SQ2 What factors should be taken into account for the decision-making process about security countermeasures?

SQ3 How can be determined to what extent a factor, found in SQ2, is present in the decision-making process?

SQ4 How can the capability level of the decision-making process about security countermeasures be determined using the created model?

1.3 Approach

The goal of creating a capability model is a design problem. This research creates an *artefact*, the capability model, in a certain *context*, in this case risk management, which is best handled with a Design Science Methodology like Wieringa (2014). In design science the main focus is solving a design problem rather then answering a research question and therefore the the research goal above is formulated as a design problem as proposed by Wieringa (2014).

Maturity capability models have been criticised for their lack of empirical foundations and to counter this a number of methodologies have been proposed. In this research the design science methodology for maturity models by Mettler (2011) is used. The design science methodology of Mettler (2011) is based on three existing design science methods for maturity capability models and is therefore firmly based in research. The method consists of four phases, also shown in Figure 1.2:

1. Define scope
2. Design model
3. Evaluate model
4. Reflect evolution

Mettler (2011) has defined decision parameters for building and testing maturity capability models for each of the four phases. These parameters can be characterised by the defined characteristics (Mettler, 2011). The overview of the parameters can be found in Table 1.1. Before the development of the capability model starts, first the need for the model needs to be established. As discussed in the previous sections, there currently is no model that assesses the capability of decision-making about security countermeasures and such a model would be added value to have more effective IS.

Table 1.1.: Decision parameters per design phase (Mettler, 2011)

1. Define scope	2. Design model	3. Evaluate design	4. Reflect evolution
Focus/breadth	Maturity definition	Subject of evaluation	Subject of change
Level of analysis/depth	Goal function	Time-frame	Frequency
Novelty	Design process	Evaluation method	Structure of change
Audience	Design product		
Dissemination	Application method		
	Respondents		

The first phase is defining the scope of the model. The focus for this capability model is providing an aid for management to review their capabilities of the decision-making process about security countermeasures. This process is a specific issue about making decisions prioritising as a group about security countermeasures. Parameters and characteristics of the capability model created in this research can be found in an overview of Appendix A.

The second phase is concerned with designing the model. This phase is divided into two steps in order to create the model.

1. Firstly, literature and existing models are reviewed thoroughly to create an overview of the relevant factors for the decision-making process about security countermeasures. This is then added upon by discussing the process with security consultants to compare the theory with practice. Scientific literature, existing maturity capability models and security consultants together provide an initial overview of the relevant factors that should be taken into account in the decision-making process of security countermeasures.

2. Secondly, a three-round Delphi study with industry experts will be carried out. A Delphi study is beneficial when seeking to combine views to improve decision-making (De Bruin and Rosemann, 2005). The first round of the Delphi study is focused on reviewing the factors found previously and collecting additional factors relevant to decision-making. Furthermore, in this first round indicators for the presence of these factors are asked to the panellists. The second round of the Delphi study is also done in the design phase. The core focus of the second round is verifying the answers of the first round and reviewing the first versions of the capability model. This provides a verified set of factors and their indicators that are relevant for decision-making about countermeasures. With this information version 1.0 of the capability model can be created as the final result of the second phase.

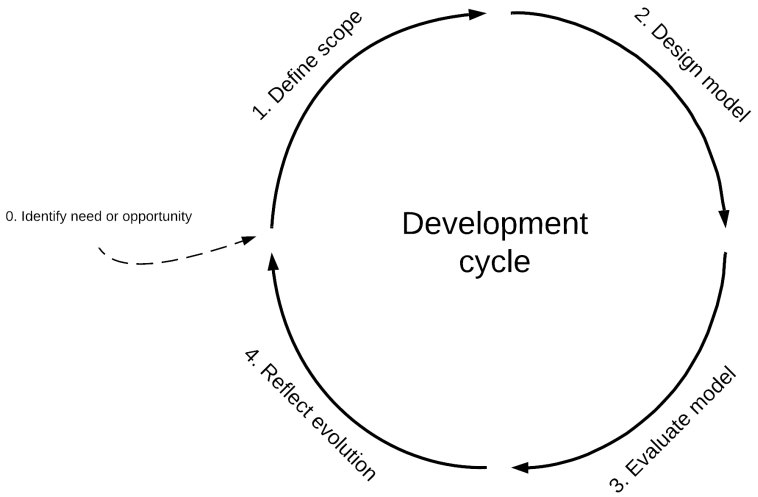


Figure 1.2.: Design science methodology for maturity models (Mettler, 2011)

In the third phase the model is evaluated. This is done by the third round of the Delphi study which includes both the industry experts and the security consultants. Furthermore, follow-up interviews with consultants are held to gain more insight into the usefulness of the model. Lastly, two case studies are carried out to reflect on the outcomes of the model. Collectively, this should provide insight into the usefulness of the capability model and give suggestions for improvement.

The fourth phase, the reflect evolution, is normally done after the model is completed and evaluated. In this phase reflection on the model and its development is done. This last phase is out of scope for this research.

In this research the first three phases are done. The main focus lies in step 2 where the model is designed. The design of the Delphi study will be described in chapter 4, but it will be a three-round study as previously discussed. The first round of the Delphi study is about identifying factors and indicators, the second round is about verifying the findings and the third round is evaluation of the model. The design of the study is shown in Figure 1.3.

1.4 Context

This research is conducted in cooperation with Northwave BV in Nieuwegein, The Netherlands. Northwave is specialised in managed security services for medium and large organisations in The Netherlands and Belgium. Northwave provides their clients with services to improve the information security of the organisation, this includes but is not limited to: cyber security tests like penetration tests, red, blue and purple teaming, 24*7 Intrusion Detection and Response Systems in a Security Operations Centre, incident response with a CERT, implementation projects for ISO27001, risk management and (awareness) training.

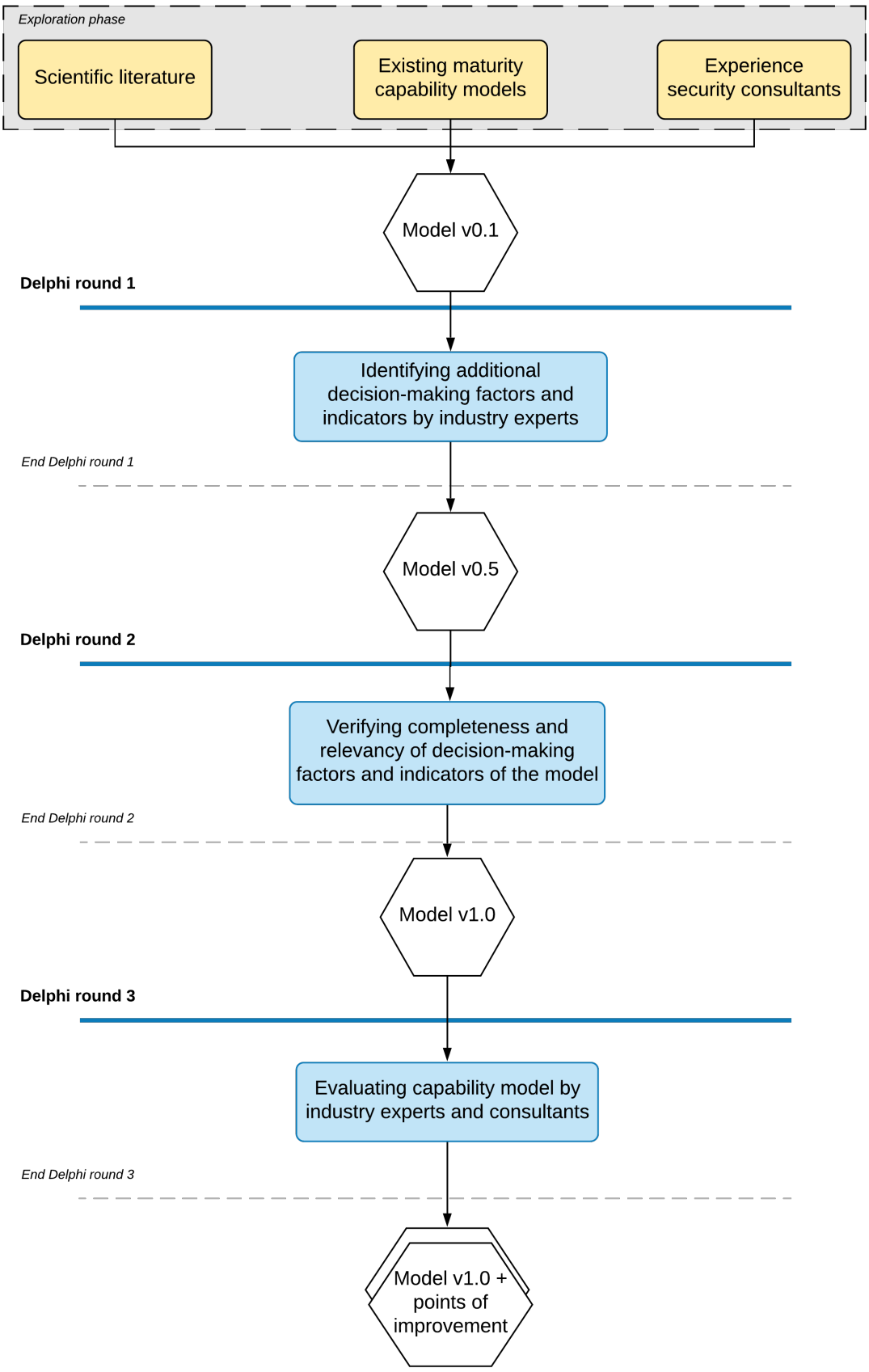


Figure 1.3.: Overview of method for capability model design

Traditionally, Northwave has been focused on providing consultancy in IS and lies the responsibility for making decisions at the organisation. However, organisations need more extensive help with IS nowadays. In order to be able to provide their customers with this help, Northwave needs further knowledge on how these organisations currently make decisions and how this can be improved. This could give Northwave an edge over the competition and be able to aid their customers better.

1.5 Structure

The structure of this thesis is build around the different phases of this development cycle. Figure 1.4 illustrates the organisation of this research mapped onto the development cycle.

Chapter 2 discusses information security and risk management more extensively. This chapter provides a general overview of risk management and how this is generally done by organisations. It shows the context of this research and where the process of making decisions about security countermeasures fits in.

Chapter 3 describes the exploration of this research. Firstly, a systematic literature review of 500 papers is conducted in Section 3.1. Afterwards, 6 maturity capability models are reviewed on factors they include in Section 3.2. Lastly, Section 3.3 identifies factors from interviews with security consultants.

The next chapter, Chapter 4, reports the Delphi study that has been conducted to test the decision-making factors in practice. The Delphi study consists of three rounds: testing the factors found (in Section 4.2), discussing the capability model (in Section 4.3) and evaluating the capability model (in Section 4.4).

This results in a full definition of the Decision-Making Capability Model for Countermeasures in Chapter 5. The chapter describes the levels and the practices in detail. In Chapter 6 the capability model is validated by interviews and case studies.

Lastly, in Chapter 7, the reliability, validity and limitations of this research are discussed. This chapter also describes possibilities for future research. The last chapter, Chapter 8, gives the conclusions of this research.

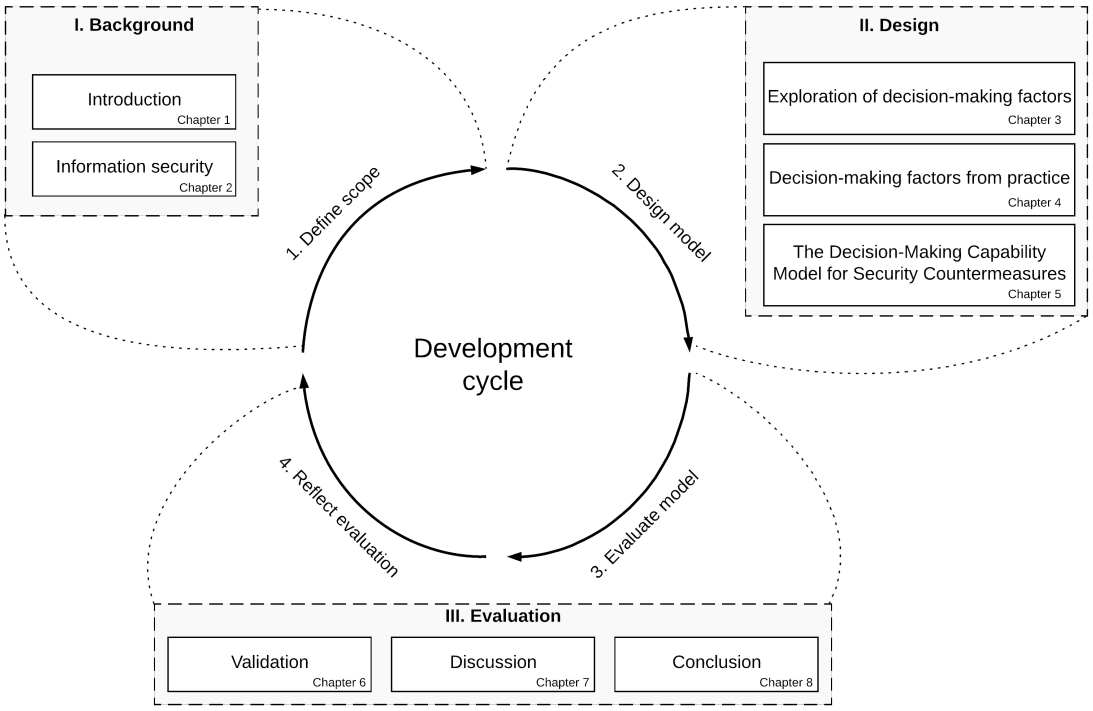


Figure 1.4.: Structure of this research

2 Information security

> *The biggest risk is not taking any risk... In a world that changing really quickly, the only strategy that is guaranteed to fail is not taking risks.*
>
> — **Mark Zuckerberg**
> (CEO of Facebook)

This chapter provides the context of this research. It discusses relevant terms and gives definitions for this research. Most importantly, this chapter shows the place that decision-making about security countermeasures has within the context of information security (IS) and risk management (RM). Firstly, IS is defined and shows essential practices to manage IS well, which provides background of this research. Afterwards, risk-based information security management is discussed to scope the research in the larger context.

2.1 Defining information security

As shown in the introduction, organisations are challenged with doing business in a changing and challenging environment. Information technology (IT) is part of the daily business in many ways. This presents challenges that have not been faced before as there was no digitisation on this scale before. Many organisations have seen that it is important to protect themselves against cybercrime / security incidents and the associated losses. Therefore, more and more organisations are managing their IS.

IS ensures that within the organisation, information is protected against disclosure to unauthorised users (*confidentiality*), improper modification (*integrity*) and non-access when required (*availability*) (ISO/IEC, 2018b; ISACA, 2012). These three aspects, confidentiality, integrity and availability (abbreviated as CIA), are mentioned as the three pillars of information security by many scholars. Torres et al. (2006) defines IS as "*a well-informed sense of assurance that information risks and technical, formal and informal controls are in dynamic balance*". This definition holds many important elements about IS. Without being well-informed and having knowledge about the organisation's status, IS is practically impossible to achieve. Controls on technology, processes and people need to be implemented to provide IS in the organisation. IS is never static. It has to be evaluated and changed dynamically and thus needs to be managed continuously.

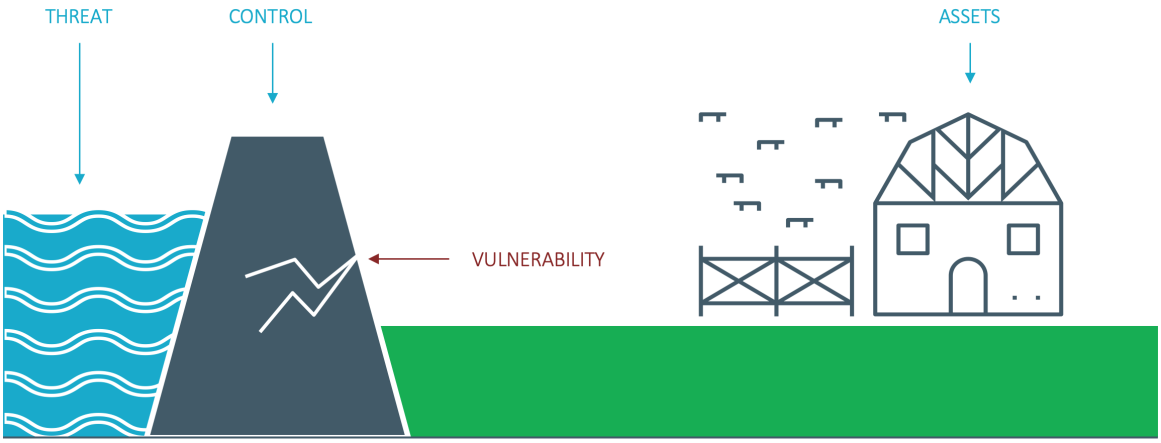


Figure 2.1.: The context of risk

The definitions of ISO/IEC (2018b), ISACA (2012) and Torres et al. (2006) hold important aspects of IS. Confidentiality, integrity and availability need to be provided by having technology, processes and people in place that ensure CIA. Confidentiality is ensuring that only people that are allowed to access the information can actually access it. This should make sure that people who should not be able to see the information cannot view it. Integrity is about the information being accurate and consistent at all times. Everywhere in the organisation the information should be the same and it should not be possible to change the information is a wrong way. Lastly, the information should be available whenever it is needed. If the information cannot be accessed, the information is of no value and thus availability of the information is important for security.

The information that the organisation is securing can be all kinds of tangible and intangible assets. An *asset* is anything that is of value to the organisation (definitions by Bojanc et al. (2012) and ISO-standard ISO/IEC (2018b)). An example is the home in Figure 2.1. An asset can be depreciated by the exposure to *threats* (the water), which are all possible events that, when turned into reality, could cause undesirable events. Treats use *vulnerabilities* (hole in the dike) in the asset to turn the threat into reality. The possible events that could impact the assets are *risks* that are described by the potential of a threat exploiting a vulnerability and thereby causing harm to an organisation. To be able to cope with the risks, organisations can take protective controls or *countermeasures* (the dike). These countermeasures could reduce the probability of occurrence or the potential impact or both. After a countermeasure the risk is still there, however it is reduced. The risk left is called *residual risk*.

Organisations have to cope with the risks and the residual risks that are facing them. Keeping the assets of the organisation secure from events threatening the CIA of the information is a challenging task. Management is tasked with providing IS to the assets and as the environment in which they operate is always changing, so is the way IS is managed.

2.2 Effective information security

IS is a complicated process of decision-making and the selection of the best security countermeasures and its implementation (Bojanc et al., 2012). For this reason there is no one right answer to have IS in place. In order to help organisations to be effective in their way of implementing IS there are a number of standards such as NIST (Stoneburner et al., 2002), COBIT (ISACA, 2012) or the ISO/IEC27001 (ISO/IEC, 2013a). In addition, research have provided organisations with numerous papers in which different models and frameworks are set out in order to aid practice (e.g. Gordon and Loeb, 2002; Cavusoglu et al., 2004; Dor and Elovici, 2016).

2.2.1 Key indicators for effective IS

According to literature there are several issues that should be addressed when implementing IS in the organisation. In 2004, Von Solms and Von Solms (2004) provided the world with 10 sins of IS. Their sins are later backed by various other authors. The number one sin according to Von Solms and Von Solms (2004) is not realizing that IS is a corporate responsibility. Number two states that IS is a business issue and not just technical. Both of these items are also stressed by Alreemy et al. (2016), Papelard and Bobbert (2018) and in the ISO27001-standard (ISO/IEC, 2013a). More key indicators for effective IS are having a good policy (Alreemy et al., 2016; Kong et al., 2012; ISO/IEC, 2013a; Von Solms and Von Solms, 2004), commitment of resources (ISO/IEC, 2013a; Papelard and Bobbert, 2018; Alreemy et al., 2016; Von Solms and Von Solms, 2004) and having a strong security culture (Papelard and Bobbert, 2018; ISO/IEC, 2013a; Von Solms and Von Solms, 2004).

It is evident that organisations should view IS as a organisation-wide issue and not just a concern for the IT department. Chief Information Security Officers (CISOs) or Security Officers (SOs) are challenged with making IS a corporate issue and getting resources to provide IS for the organisation. Fear, uncertainty and doubt have traditionally been drivers to invest in security management (Cavusoglu et al., 2004) and therefore to guarantee resources. The way IS is managed affects many aspects of the organisation. This includes the organisations' competitive advantage, customer satisfaction, the ability to comply with legal and regulatory demands, the ability to manage risks, and more (Dor and Elovici, 2016). Still, IS is not the core business of the organisation and thus is only a means of securing the business-as-usual.

2.2.2 Quantifying IS

Costs for securing business-as-usual should be kept as low as possible to gain bigger profits. In order to keep an eye on these costs, organisations want to know where they stand on the effectiveness of their investments. Gordon and Loeb (2002) show that investments in IS will not be more effective when spending more than 37% of the loss of a potential security breach. Their conclusions mark the start of quantifying IS.

Kajava and Savola (2005) stressed that more metrics and measurements should come for IS. They conclude that having measurements in place provides evidence of the level of IS in the organisation, it provides support at audits and shows conformance of security policies and reality. Most importantly, they conclude that "*standard methods to offer feedback for decisions are needed*" (Kajava and Savola, 2005).

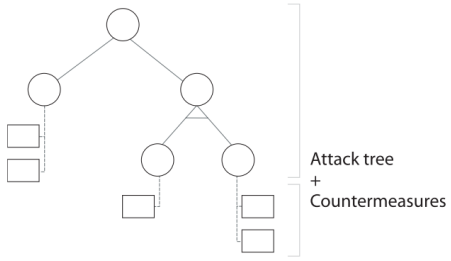
Several methods to evaluate security investments have been introduced over the past years. In line with the Return on Investment-formula from finance, the Return on Security Investment (ROSI) metric has been produced by Sonnenreich et al. (2006). The ROSI-metric describes how much of the risk is mitigated by a certain solution, see Equation (2.1). ROSI applies the Single Loss Exposure and Annual Rate of Occurrence to be able to quantify the risk mitigated and with this it becomes a relevant metric. On the other hand there is the Return on Attack (ROA), see Equation (2.2) which provides insight in what brings most value to the attacker (Cremonini and Martini, 2005). Both provide indicators which countermeasure for IS are relevant to take as they show which measure provides the most value to either the defender or the attacker.

$$ROSI = \frac{(risk\ exposure \times \%\ risk\ mitigated) - solution\ cost}{solution\ cost} \tag{2.1}$$

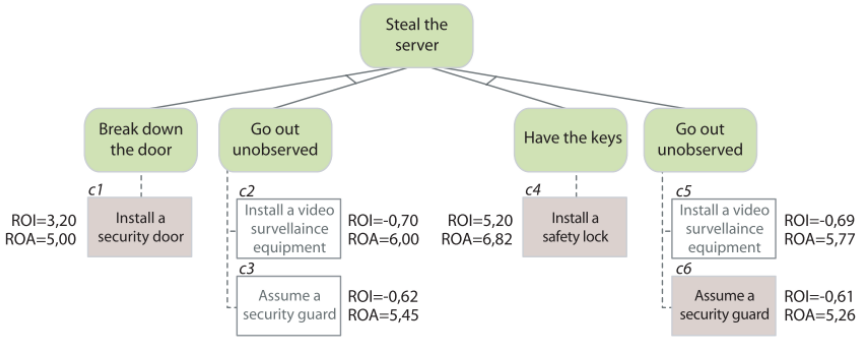
$$ROA = \frac{gain\ from\ a\ successful\ attack}{cost\ before\ security\ measure + loss\ caused\ by\ security\ measure} \tag{2.2}$$

Combined the ROSI and ROA metrics are used by Bistarelli et al. (2006) in defence trees. In doing so, it easily shows what measures are worth investing in by the defender and which actions are worth attacking for the attacker. An optimal investment can be found using the ROI and ROA in a defence tree. An example of the defence tree can be found in Figure 2.2. This figure shows that installing a security door, installing a safety lock and assuming a security guard are the most cost-efficient measures as they have the highest ROI and the highest ROA. Together, these three countermeasures cover all the possible attacks to steal the server and are therefore effective in providing IS.

There are numerous other metrics and aids in evaluating and making decisions in IS. For example Mean Failure Costs (Rjaibi et al., 2013), game-theoretic models (Cavusoglu et al., 2004; Panaousis et al., 2014) and real options (Gordon et al., 2003; Daneva, 2006) are introduced in the field of IS. All of these methods could help security professionals in evaluating the IS and make decisions to improve IS in their organisation. Unfortunately, starting to use these metrics can be difficult as there is no data available. This could prove to provide a lot of overhead, but according to standards (ISO/IEC, 2013a) it is worth investing in this to rationally improve IS.



(a) Defence tree (Bistarelli et al., 2007)



(b) Example annotated defence tree (Bistarelli et al., 2006)

Figure 2.2.: Defence trees

2.3 Risk-based information security

Taking a risk-based approach to IS is stressed by almost all authors writing about security (e.g. ISO/IEC, 2013a; Papelard and Bobbert, 2018; Von Solms and Von Solms, 2004; Alreemy et al., 2016; Kong et al., 2012). Identifying what the threats to the organisation are and how their assets should be protected, is vital to minimize the risk to the organisation.

The entire process of thinking about the assets, threats, vulnerabilities, risks and countermeasures is called *risk management* (RM) which is also done in the field of IS. Most organisations use a risk-based approach for remaining in business. RM is one of the core parts of maintaining safety, physical security and cybersecurity in an organisation. To manage IS risks properly, a number of standards have been developed, for example by the International Organisation for Standardization (ISO) together with the International Electrotechnical Commission (IEC) (ISO/IEC, 2013a) or by the American National Institute of Standards and Technology (NIST) (Stoneburner et al., 2002). These standards aim to provide organisations with easy-to-use processes and checklists to conduct RM in the field of IS well. A lot of organisations (almost 100 organisations in The Netherlands in 2017[1]) are even certified for the information security management system standard, ISO27001, to show they have an Information Security Management System (ISMS) in place. To maintain the quality the ISMS, a risk-based process is provided by ISO/IEC in the standards 9001 and 31000. This process consists of four simple steps: Plan, Do, Check and Act (ISO/IEC, 2018a). This process is shown in Figure 2.3.

[1]ISO - `https://isotc.iso.org/`

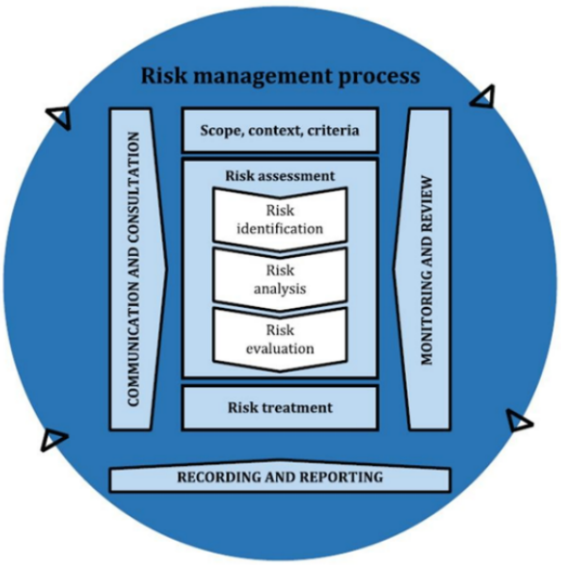


Figure 2.3.: Risk management process (ISO/IEC, 2018a)

Within the scope of the ISMS of an organisation, RM is conducted. The process of managing risks by ISO/IEC-standard 31000 (ISO/IEC, 2018a) uses this PDCA-cycle of ISO9001 (ISO/IEC, 2015). The '*plan*'-phase of the cycle is the most substantial part, especially the first time the cycle is done. The first time it demands the context, scope and requirements of the ISMS. Afterwards, it needs to be operated, monitored and reviewed and lastly it needs to be maintained and improved (ISO/IEC, 2018b). The plan-phase is important for the entire management cycle as this provides insight in the context of the ISMS, the current threats, risks and the countermeasures that need to be taken so they can be managed in the later phases.

Typically, there are three major steps in the planning phase:

1. Determine the scope and context of the ISMS and set criteria for the ISMS
2. Do risk assessment
    a) Identify risks
    b) Analyse the risks
    c) Evaluate risks
3. Produce risk treatment plan

In the Do, Check and Act steps of the PDCA-cycle the planning is carried out as well as possible. The ISMS is implemented and maintained by using the appropriate controls from the standard ISO/IEC27001 ISO/IEC, 2013a and the best practices ISO/IEC27002 (ISO/IEC, 2013b). This research is focused on how spending on security should be done and therefore the planning phase is the primary focus. The next paragraphs go into more detail about the RM-process.

2.3.1 Context of the ISMS

The first step is understanding the context of the information security management system. Without knowing the context of the organisation and more specifically the ISMS, it is not possible to identify the relevant threats, vulnerabilities and people who will manage the risks. The approach for implementing IS initiatives will be different for every enterprise. Organisations could make use of COBIT5 for Information Security (ISACA, 2012) in order to fully understand their context. The organisation needs to determine the external and internal parties that are relevant to the purpose of the ISMS (ISO/IEC, 2013a). Of those parties, the expectations and requirements should be identified, because this indicates the scope of the ISMS. The scope of the ISMS then is determined and documented, so it can be referred to. The scope includes the external and internal parties relevant to the ISMS and the requirements that they have towards the ISMS.

The leadership should be committed to implement the ISMS as IS touches upon many aspects of the organisation. The main aspect of the commitment of leadership is instating an IS policy. This policy should be appropriate to the purpose of the organisation and includes the security objectives, the commitment to satisfy applicable requirements and commitment to continual improvement of the ISMS (ISO/IEC, 2013a). This policy should be documented and communicated to the entire organisation and even available to interested parties. The leadership should also make resources available for an effective ISMS and steer and reflect on the outcomes of the ISMS to be able to continuously improve the ISMS. Of course, the leadership does not have to do this themselves, but they can assign roles, responsibilities and authorities to people within (or even outside) the organisation to make sure the ISMS is effective.

2.3.2 Risk assessment

Knowing the context of the ISMS, the next step is to assess the relevant risks. The risk assessment step consists of three sub-steps: risk identification, risk analysis and risk evaluation. Together these steps provide the possibility to draft a risk treatment plan. Risks can be identified on several levels, for example there are strategic risks, like '*customer data could become publicly available*' or operational risks such as '*this production line could be shut down because of a malfunction*'. On all the different levels risks should be identified and the risk owner has to be known. Only then the organisation can manage their risks properly.

Risk identification

Identifying the risks within the scope of the ISMS is a cooperative process. Every person, every stakeholder, has a different view risks and which risks there are most relevant for the organisation. Therefore, it is crucial that risk identification is done by a group of people from different backgrounds. That provides insights from all sides of the organisation and produces a full risk identification.

During risk identification, the vulnerabilities of the organisation are determined and the threats outside of the organisation are listed. The set of control objectives of the Annex A of ISO/IEC27001 (ISO/IEC, 2013a) can also be used for finding the risks applicable. As well as identifying the risks, the *risk owners* should be identified as well. The risk owner is responsible for the risk and for the possible countermeasure(s) taken to reduce the risk.

Risk analysis

The risk analysis step looks into each risk in more detail to make it possible to quantify the risks. However, before the risks can be analysed it needs to be established what the risk acceptance criteria are (also called the *risk apatite*) and what the criteria the risks are measured against. Often, this is done by setting op a risk matrix with the levels *high, medium* and *low* on two axes: impact (potential loss) and chance (likelihood of occurrence) (ISO/IEC, 2013a). The potential consequences or potential loss that would result from the risk needs to be quantified, preferably in a monetary value. This provides known quantification that the entire organisation understands. A realistic probability of the occurrence of the risk should be identified as well. Similar to identifying the risks, determining the probability of occurrence is seen by every stakeholder differently. Therefore, it is vital to discuss the probability in a group as well and set a likelihood collectively. Together, the impact and the likelihood determine the risk. Generally, this is determined with the formula below, Equation (2.3).

An example risk matrix is shown in Table 2.1. In this table, the risks that are accepted are coloured green (down-left corner) and the ones that cannot be accepted and have to be treated are coloured in red (upper-right corner). Regularly, the levels are quantified by the organisation. For instance, a high chance is '*occurs daily*' and a high impact indicates a potential loss of '$>$ *€250.000*'. A risk such as '*The vital information systems are down because of a DDoS-attack*', will be faced daily by most banks and the potential impact is far more than €250.000, thus this risk is placed in the upper-right corner of the risk matrix.

$$Risk = probability \times potential\ loss \tag{2.3}$$

Risk evaluation

When the criteria are set and the quantification of the risks is done, the risks can be evaluated. This leads to a filled-in risk matrix with all identified risks. As the risk apatite is identified before, this instantly shows what risks are accepted and which are not. Frequently, this leads to new discussions about the quantification of certain risks as some stakeholder might not accept the risk at all. This can be altered to provide an even better evaluation. Accepting the risk is one of the options that decision-makers have to cope with risk. All the options according to Bojanc et al. (2012) are:

Table 2.1.: 3×3 Risk matrix

Impact / chance	Low	Medium	High
High			
Medium			
Low			

- **accepting** the risk;
- **reduction** of the risk by investing in an appropriate countermeasure;
- **transfer** the risk (e.g. to an insurance agency); and
- **avoidance** of the risk by limiting or close the service.

Selecting the appropriate strategy to accept, reduce, transfer or avoid the risk is difficult. There are a few scholars which aid making selecting the right strategy by providing quantification or by creating a decision-making process such as Bojanc et al. (2012). Figure 2.4 provides a decision-making flowchart to select the best strategy according to Bojanc et al. (2012). This flowchart needs some inputs, such as the risks, risk apatite and the budget. With these inputs that are determined in the risk analysis-step, one can easily determine the appropriate strategy by using the criteria set previously. Afterwards, the risks should be prioritised on which are needed to tackle first. A list with all risks is a deliverable of the risk assessment-step. This includes all risks that are accepted, transferred or avoided together with actions that are (or need to be) taken. Furthermore, a prioritised list of risks that need to be reduced is provided as input for a risk treatment plan.

2.3.3 Risk treatment

Now that the risk assessment is done and a prioritised list of risks is created, the treatment plan for the risks can be formulated. In the Annex A of the ISO-standard 27001 (ISO/IEC, 2013a) a number of security countermeasures are formulated that can be used to reduce the risks. The standard 27002 (ISO/IEC, 2013b) provides best practices in how to implement those countermeasures.

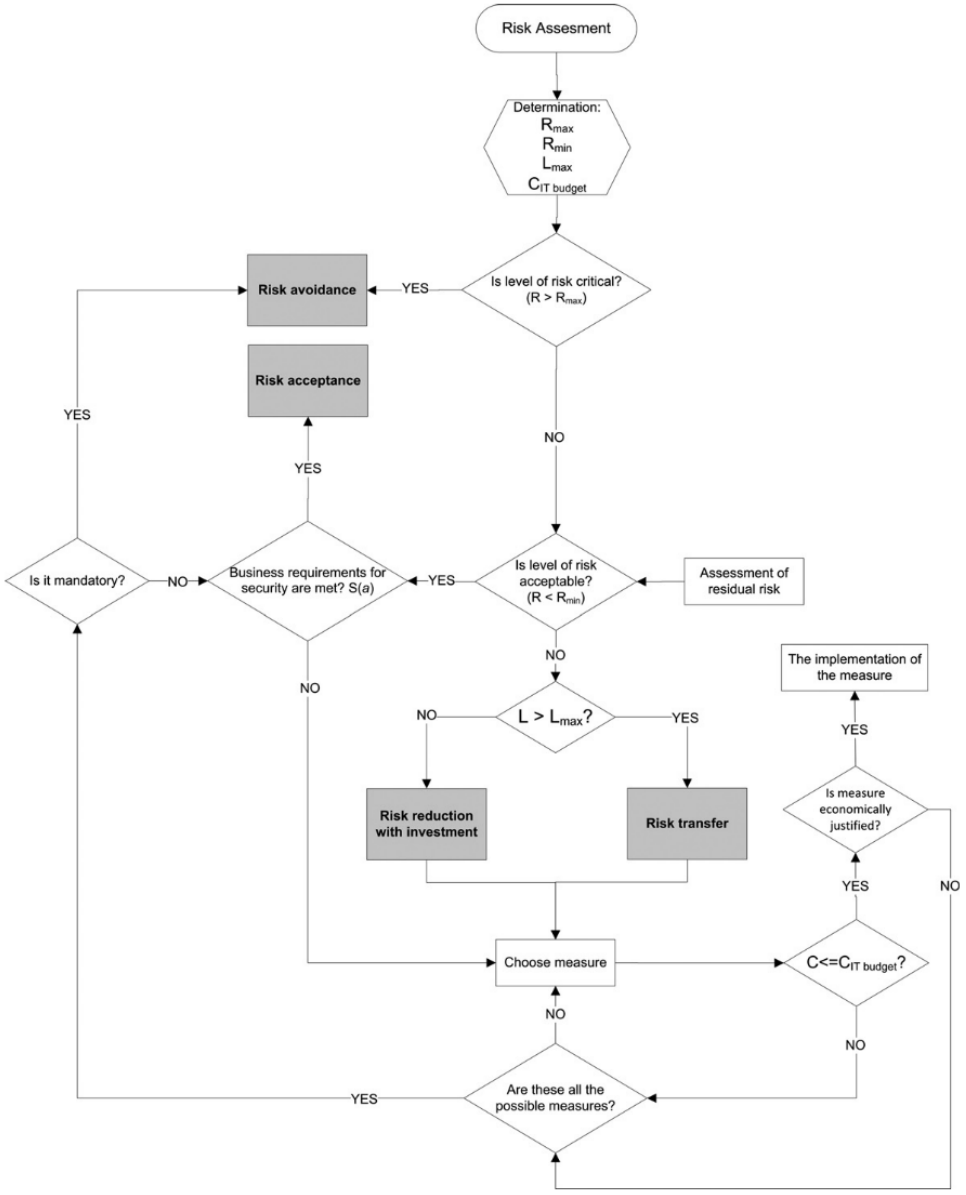


Figure 2.4.: Selection of risk reduction strategy (Bojanc et al., 2012)

Even though there are 114 countermeasures available in 35 main security categories, finding the appropriate countermeasures is a challenging process which is not described in the ISO-standard. According to Fenz et al. (2011) and Ekelhart et al. (2009) there are many alternatives to choose from, but it provides little intuitive decision support. There should be a more sophisticated decision-making approach should be created (Bojanc et al., 2012) and this approach should help the security practitioner in accomplishing his or her tasks (Dor and Elovici, 2016).

Currently, the ISO-standard states that the organisation should compare the countermeasures and choose the ones that are relevant. This results in a *Statement of Applicability* that contains all necessary countermeasures and the justification for inclusion and exclusion for the measure (ISO/IEC, 2013a). Next to the statement of applicability, a risk treatment plan is formulated

on how the countermeasure will be implemented. For the countermeasures described in the Annex A of ISO27001, a proposed way of implementing the countermeasure is delivered in ISO/IEC27002 (ISO/IEC, 2013b). Finally, the risk owners should accept the residual risk that is left after the countermeasure is in place and this should be well documented.

All this information concludes the '*Plan*'-phase of the PDCA-cycle and starts the '*Do*'-phase in which the countermeasure can be implemented. The entire ISMS should be updated continuously to reflect the current situation, as there could be new suppliers which could for example bring new risks that need to be accepted, reduced, transferred, or avoided. The ISMS is constantly adapting to the current situation, which is generally done by following the cycle on a yearly basis.

2.4 Decision-making process about countermeasures

Information security needs to be managed continuously to ensure the confidentiality, integrity and availability of the organisation. The assets of the organisation should be protected from threats in order to cope with risks to the business. There are standards, such as ISO27001 (ISO/IEC, 2013a), that provide guidance to manage IS well. Risk management is part of this management of IS. RM is an aid to identify, analyse and evaluate the risks to the organisation.

Risks to the organisation are identified, analysed and evaluated. Among risks that are risks that are accepted, transferred or avoided, there are also risks that need to be reduced. Risks that need to be reduced should be mitigated by a countermeasure in order to reduce this risk to an acceptable level. The ISO27001 and ISO27002 (ISO/IEC, 2013a; ISO/IEC, 2013b) give guidance on how this treatment should be done, but research has shown that there are a lot of alternatives to choose from which makes choosing difficult. Furthermore, there is no clear process of choosing the countermeasure. Decision-making about taking security countermeasures that reduce the risk is a difficult process. This process is part of treatment of the risks within risk management.

Part II

Design

3 Exploration of decision-making factors

> *For me, it is always important that I go through all the possible options for a decision.*
>
> — **Angela Merkel**
> (Chancellor of Germany)

To create a capability model to assess the decision-making process about countermeasures, the challenge is knowing what factors are relevant to decision-making in this context. In this chapter the academic side of decision-making about countermeasures is reviewed. This chapter explores literature and existing models in order to gain a first insight in important decision-making factors about countermeasures.

In order to find the relevant factors this chapter looks into three kinds of sources: *literature*, *existing maturity capability models* and *security consultants*. In section 3.1 a systematic literature review (SLR) is carried out, which included 500 papers. Afterwards, in section 3.2, 6 existing maturity capability models are reviewed for factors of decision-making about security countermeasures. This is added upon with insights from practice. Interviews with 5 security consultants, who have seen what factors are important in multiple organisations, are used to explore the practical side. In sections 3.4 and 3.5 a summary of all decision-making factors found is presented and the implications for the rest of the research are discussed.

3.1 Factors from literature

The first exploration is done with reviewing scientific literature. Current literature can provide insight in the already identified factors that are essential in decision-making about security countermeasures. To create a good overview of the factors provided in literature, a systematic literature review is carried out. A systematic literature review (SLR) is a means of identifying, evaluating and interpreting all available research to a particular research question, or topic area, or phenomenon of interest (Kitchenham, 2004). As to the best knowledge of the author no review paper about the factors of decision-making in IS is available, a SLR is a good method to identify the all factors in current research for decision-making about countermeasures in IS.

3.1.1 Methodology

To conduct the systematic literature review the methodology as described by Kitchenham (2004) is used. Her research is based on three existing guidelines for conducting SLRs and is widely used in the academic world. According to Kitchenham (2004), the SLR consists of three stages: (1) planning the review, (2) conducting the review and (3) reporting the review. This section report the SLR that is carried out.

Review protocol

With this SLR the factors for decision-making about countermeasures in IS should be identified. The core question in the SLR is the second sub-question of this research: *'What factors should be taken into account for the decision-making process about security countermeasures?'*.

In this search five databases are used as input: Google Scholar, Scopus, IEEE, Web of Science and ACM. In addition some papers are added that have come from recommendation by supervisors and Mendeley. To search the databases the following keywords are used, see Table 3.1. This resulted in the following search query:

```
("success factor" OR "critical factor" OR CSF) AND ("decision-
making" OR decision OR governance) AND (security OR "IT risk" OR
"information security" OR cybersecurity OR "cyber security")
```

Inclusion & exclusion criteria

Literature found with these keywords is reviewed with specific inclusion and exclusion criteria (see Table 3.2). First these criteria are used to select literature based on the title. Then, of the remaining papers the abstract is reviewed with the same inclusion and exclusion criteria.

Identification of research

The selection using the in- and exclusion criteria above has lead to the following process, see Figure 3.1. For Google Scholar the first 20 pages of results are reviewed (200 results). Of all other sources the results are reviewed in full. Upon reviewing the collected papers in full, four papers could not be accessed and are therefore left out the SLR. In Table B.1 in Appendix B the final list of included papers can be found.

Table 3.1.: Keywords used in SLR

Factor	Decision-making	Security
Success factor	Decision	IT risk
Critical factor	Governance	Information security
CSF		Cybersecurity
		Cyber security

Table 3.2.: Inclusion & exclusion criteria of SLR

Inclusion criteria	Exclusion criteria
Success factors of decision-making in risk management Implementing information security management	Papers that are not in English Only one of the search items reflected Adoption of a kind of technology (like cloud) Information needs for governance (plain) IT governance Policy and security of nations Development of a metric

Extraction of data

Nineteen scientific papers are found in the SLR. These papers are read in full and from this, 3 papers where excluded from the results as they did not offer decision-making factors about countermeasures. The remaining 16 papers are also read in detail to collect the factors that are relevant for decision-making about countermeasures in risk management.

During extracting the data, not all factors mentioned in the articles are included in this research. The reason for this is that most papers are about critical success factors of RM or IS in general. Not all factors which are relevant in risk management or information security, are relevant for decision-making about countermeasures.

Excluded are the aspects:

- **Staff awareness and training.** The awareness itself is a countermeasure to create a more security organisation. Therefore, this is not a factor that has to be taken into account when making a decision. Having more awareness training could be the outcome of the decision.
- **Influence of third parties.** Third parties do not influence the decision of the organisation. It does have influence on the effectiveness on the IS as a whole, but not on the decision-making process.
- **Leadership by example.** A factor for the effectiveness of IS in an organisation mentioned multiple times is the example that the leadership sets. As this is about how the leadership is coping with the countermeasures put in place, this is not a factor to take into account for decision-making.
- **Culture and policies of the organisation.** Although the culture and policies of the organisation could impact the way a decision is made, it does not have an impact on which decision is made. Therefore, the culture and available policies are not taken into account as factors.

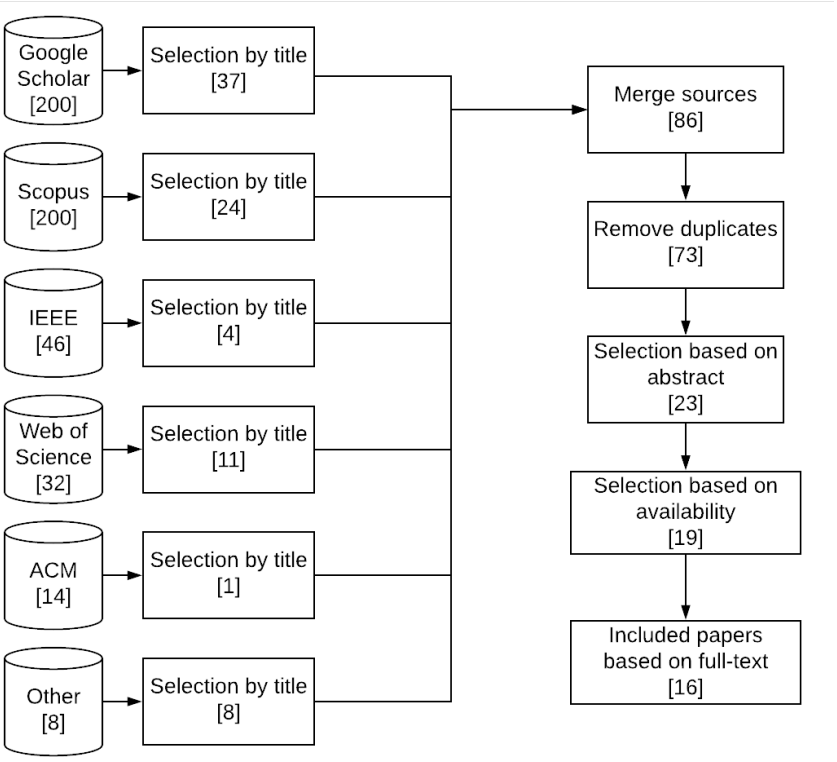


Figure 3.1.: Papers collected through systematic literature review

3.1.2 Results

From the 16 papers in the SLR, 8 relevant factors for decision-making about countermeasures are identified. Table 3.3 presents the overview of the factors from literature. The references are IDs that can be found in Table B.1 in Appendix B on page 106. To find these eight factors, all factors mentioned in the sixteen papers in the SLR are cited. Appendix B shows the exact quotes of the factors from literature and the classification of the factor in a category in Table B.2. These categories are used in the table below, Table 3.3, as the factors from literature.

The most mentioned factor in literature is '*Use quantifiable measurements for evaluation of the countermeasure*'. Almost all papers found describe in one way or another that it is important to base decisions of security on measurements. Some focus more on measuring to evaluate the performance of the security (L01, L03, L04, L07, L09, L10, L16). Others state measuring security helps in decision-making (L15) or in enforcing the security in the organisation (L17).

Further important factors are the fit of the countermeasure in the business context and the backing a countermeasure has in the organisation. Both of these factors are mentioned by most papers as very important factors for effective IS. Without aligning security with the business the security cannot be effective for the organisation. Security should always be viewed as an enterprise-wide issue (L05, L07, L14, L15) and be aligned with the strategic

goals of the organisation (L01, L02, L09, L14, L19). The countermeasure needs to be in line with the strategic goals of the organisation.

In addition, the countermeasures need to have backing in the organisation to be effective. Without top managements support there will be no effective IS in the organisation, all of the literature that mentioned this factor agrees with this. The support of the management could mean that sufficient funding and resources are allocated to security, which is another factor that is mentioned in literature. Not only funding in money (L01, L02, L09, L19), but also the right people and empowering of those people are needed for effective security (L11, L12 L17, L18) needs to be taken into account when choosing a countermeasure. Furthermore, assigning responsibility of the countermeasure determines the effectiveness of the security as well (L03, L11, L14, L19).

According to the majority of scholars, IS should be based on risks. A countermeasure should always reduce a risk. Some mention defining a risk apatite (L03, L11), others focus more on the assets of the organisation (L11, L16). But most just state that risk management is critical for effective IS (L01, L07, L09, L10, L12, L17). A number of the the scholars add to this by stating that following standards and frameworks to manage risks helps to manage IS well. Countermeasures that are described in best-practices could then offer effective measures.

Lastly, in the environment of the organisation a lot will happen. An organisation should learn from incidents in their own organisation or from others (L12, L15) and they should act upon those lessons learned (L03, L18). In line with this the countermeasures should prevent the incidents that happened before from happening again.

Table 3.3.: Factors found in literature with reference

Factor	Reference
Use quantifiable measurements for evaluation of the countermeasure	L01, L03, L04, L07, L09, L10, L11, L12, L15, L16, L17
Fit countermeasure in the business context	L01, L02, L05, L07, L09, L11, L12, L14, L15, L17, L19
Get backing for the countermeasure	L01, L03, L05, L09, L11, L12, L14, L15, L17, L18, L19
Reduce a risk with the countermeasure	L01, L03, L07, L09, L10, L11, L12, L16, L17
Choose countermeasures from best-practices	L01, L07, L09, L10, L12, L14, L15, L16, L17
Take the available resources into account (funding and knowledge)	L01, L02, L09, L11, L12, L17, L18, L19
Assign responsibility of the countermeasure	L03, L05, L11, L12, L14, L19
Choose countermeasures that prevent previous incidents	L03, L12, L15, L18

3.2 Factors from maturity capability models

The second source of information in the exploration phase are existing maturity capability models (MCM). These models combine academia and practice and are therefore a valuable source of information for decision-making factors about countermeasures. Existing maturity capability models review important factors in other application areas. These same factors could also be of influence of decision-making factors about countermeasures in IS.

In this search of decision-making factors in existing MCMs a number of models have been viewed. Many of them have their origin in the Capability Maturity Model of Paulk et al. (1993). These MCMs have been used in multiple application areas where they have shown their value. The search has confirmed that there is no capability model that has the same aim as the model created in this research, being to produce a performance indicator of the decision-making process about countermeasures in IS.

3.2.1 Methodology

In the search for existing MCMs multiple sources are used. Firstly, Google Scholar and Scopus are used to search for models. Terms used in the search where `"maturity model"`, `"information security"`, `"IT governance"` and `security`. This provided a number of results of which just a few MCMs were relevant to review. In addition to the search on the internet, there were a number of maturity models recommended by practitioners which were reviewed on their applicability for this research. Ultimately, the set of MCMs is chosen based on the following inclusion and exclusion criteria, see Table 3.4.

Using these inclusion and exclusion criteria 6 MCMs are included. The included models are: CMMI (CMMI Product Team, 2010), COBIT 5 (ISACA, 2012), C2M2 (Christopher et al., 2014), ISMM (Saleh, 2011), MMGRSeg (Mayer and Fagundes, 2009) and SIM3 (Stikvoort, 2010). These models have different levels of abstraction and therefore provide an overview of the different decision-making factors that are taken into account by the MCMs. The CMMI

Table 3.4.: Inclusion & exclusion criteria of MCMs

Inclusion criteria	**Exclusion criteria**	*e.g.*
Widely used in practise	Completely no documentation freely available	CMMI v2.0
Provide insights in overall process OR in a specific area of IS	Only review software	SSE-CMM
	Focus on a community rather then one organisation	CCSMM
	Not aimed at improving efficiency and effectiveness	
	More of a methodology then a maturity model	ISM3

model for example, can be used for the development of any product or service, whereas the SIM3 model is used on a very specific part of IS, namely the incident response.

After selecting the maturity capability models, the models are compared. Unfortunately, there is no clear way in which MCMs can be valued and evaluated (Hillegersberg, 2019). As there is no standard way in literature to evaluate the MCMs, a combination of elements of the paper by Mettler (2011) and Pöppelbuß and Röglinger (2011) will be used. The selection of elements is done by valuating the different elements on their use and information for this research. The elements that will be taken into account in this evaluation are:

- Applicability
  - Origin
  - Reliability
  - Practicality
  - Accessibility
  - Application method
- Design principles
  - Application domain
  - Purpose of use
  - Target audience
  - Definition of maturity levels

The extraction of the decision-making factors is done during the evaluation the MCMs. The different MCMs look at many different factors of which not all are relevant in the context of this research. The factors that are included are factors that have to do with decision-making and evaluation of different options. This came down to the same inclusion criteria of factors as used in the literature review. In this review of MCMs the aspects like staff awareness and training, influence of third parties and leadership by example are also excluded.

3.2.2 Comparing maturity models

CMMI for Development, v1.3

The Capability Maturity Model Integration for development has its basis in the capability maturity model of Paulk et al. (1993). It provided guidance for applying CMMI best practices in a development organisation (CMMI Product Team, 2010). The model focuses on activities for developing quality products and services by describing the different levels in which the product or service could be in. The model look into three dimensions: (1) procedures and

methods defining the relationship of tasks, (2) tools and equipment and (3) people with skills, training and motivation. These dimensions are all integrated by the processes of an organisation. Therefore, creating quality processes helps the organisation to maximise the potential of the three dimensions.

CMMI-DEV is divided into 22 process areas (CMMI Product Team, 2010). Not all of the areas are relevant to this research as they describe the entire range of processes that are present in a development organisation. The process areas to which attention are given, are: (a) Decision Analysis and Resolution, (b) Measurement and Analysis, (c) Organisational Performance Management, (d) Organisational Process Performance, (e) Process and Product Quality Assurance, (f) Quantitative Project Management and (g) Risk Management.

Currently, version 1.3 of CMMI-DEV is not the newest version available. After 8 years of no updates on the maturity model, version 2.0 was released. However, CMMI 2.0 is not publicly available for free. Therefore, this model is not reviewed, but the older version 1.3 is used in this research.

COBIT 5

The models of Control Objectives for Information and Related Technologies (COBIT) have been around for a long time (ISACA, 2012). The COBIT 5 framework consists of multiple components for different application areas. In this research the COBIT 5 for Information Security is reviewed. The COBIT framework is based on five principles, as shown in Figure 3.2. With these principles COBIT looks into 7 enablers:

1. Principles, policies and frameworks
2. Processes
3. Organisational structures
4. Culture, Ethics and Behaviour
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competences

The relevant parts of COBIT 5 for this research are in the enablers 1, 5, 6 and 7. It should be noticed that COBIT 5 is not fully available for free and that the documents to review the model are free to view documents provided by ISACA to get to know COBIT 5. Unfortunately, this model could not be investigated in detail because of this.

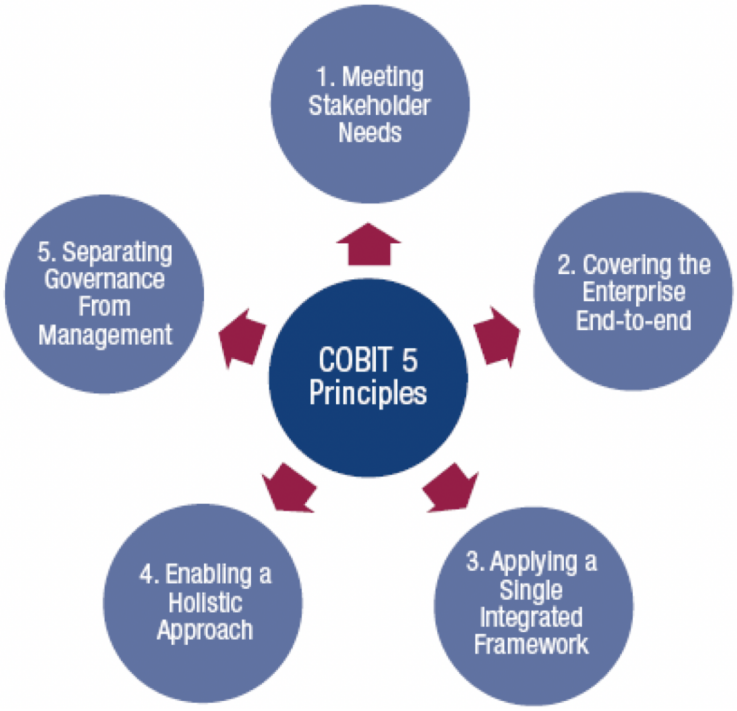


Figure 3.2.: COBIT 5 Principles (ISACA, 2012)

Cybersecurity Capability Maturity Model - C2M2

The Cybersecurity Capability Maturity Model, C2M2, has been developed by the Department of Energy of the United States (Christopher et al., 2014). The model combines aspects of existing cyber security standards to help develop the cybersecurity capabilities of an organisation and is easily integrated with NIST (Stoneburner et al., 2002). C2M2 is presented on a high abstraction level so it can be adopted by various organisations with all different kind of sizes.

The C2M2 model is divided into 10 domains and each domain is a grouping of a cybersecurity practices. The domains are: (1) Risk management, (2) Asset, Change, and Configuration Management, (3) Identity and Access Management, (4) Threat and Vulnerability Management, (5) Situational Awareness, (6) Information Sharing and Communications, (7) Event and Incident Response, Continuity of Operations, (8) Supply Chain and External Dependencies Management, (9) Workforce Management, and (10) Cybersecurity Program Management. Like with the previous two models, not all domains are relevant. This research focused on the domains 1, 4, 5, 7, 9 & 10.

Information Security Maturity Model - ISMM

The Information Security Maturity Model by Saleh (2011) has been developed to build-in security in an organisation. The model consists of four domains: organisation governance, organisational culture, the architecture of the systems, and service management. Together, these domains provide insight in how well the organisation is compliant to the security objectives set by the organisation.

To measure the level of compliance in the four domains, a questionnaire has been developed by Saleh (2011). In this short questionnaire, the organisation can find out the level of compliance and therefore identify the next steps it can take to get more mature in IS management.

Risk Management Maturity Model in Information Security - MMGRSeg

The Risk Management Maturity Model in Information Security, MMGRSeg, aims to provide insight in the risk management method of the organisation (Mayer and Fagundes, 2009). The model is build on best practices and previous maturity models like CMMI and COBIT. Furthermore, MMGRSeg is fully aligned with the ISO standard ISO27001 for information security management. The maturity levels of the model are similar to the levels of the CMMI and are shown in Figure 3.3 to provide insight in how these model work.

The MMGRSeg focuses on the activities carried out in risk management: context definition, risk analysis/assessment, risk treatment, risk acceptance, risk communication, and monitoring and critical risk analysis. Within each of these activities tasks are described of which the maturity level can be determined. All of the activities of the MMGRSeg are in one way or another relevant for this research.

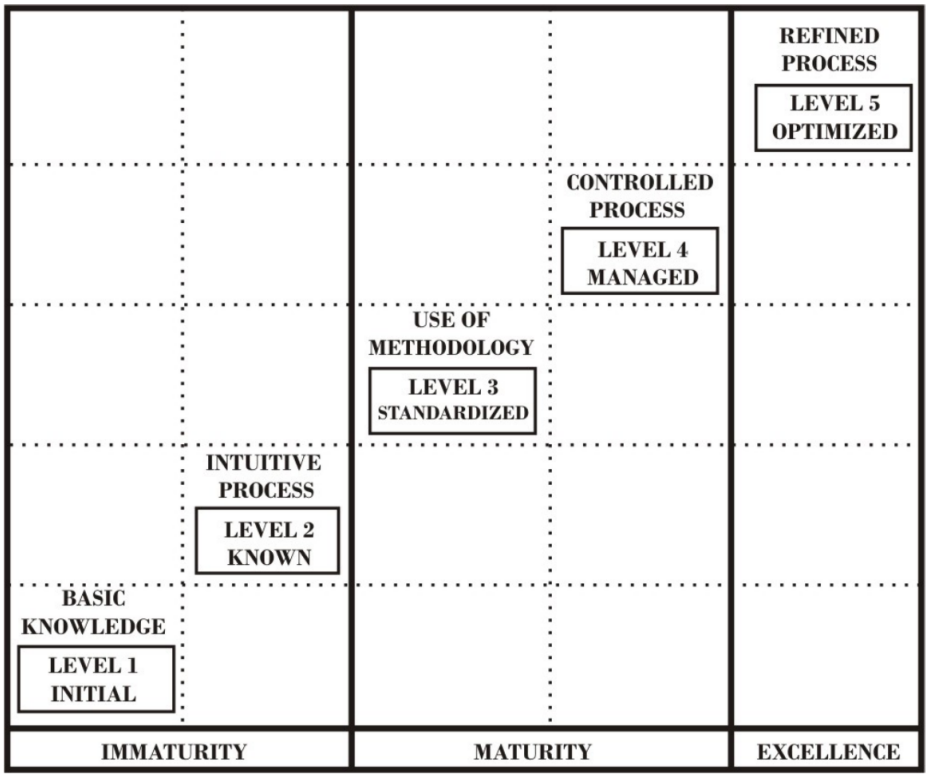


Figure 3.3.: Maturity levels of MMGRSeg (Mayer and Fagundes, 2009)

Table 3.5.: Comparison of maturity models

	CMMI MCM1	**COBIT 5** MCM2	**C2M2** MCM3	**ISMM** MCM4	**MMGRSeg** MCM5	**SIM3** MCM6
Applicability						
Origin	Academic	Academic	Practice	Academic	Academic	Practice
Reliability	Validated	Validated	Untested	Untested	Verified	Verified
Practicality	General	General	Specific	General	Specific	Specific
Accessibility	Free/paid[a]	Paid	Free	Free	Free	Free
Application method	Certified professionals	Certified professionals	Self-assessment	Third-party assisted	Self-assessment	Third-party assisted
Design principals						
Application domain	Development of products and services	Enterprise governance on IT	Cybersecurity management	Information security management	Risk management	Security incident management
Purpose of use	Assessment of products and services	Improving governance in the organisation in relation to IT	Measure and improve the security program	Ability to achieve the security goals	Assessment of risk management process for IS	Assessment of the incidence response protocol
Target audience	Multiple	Multiple	Security managers	Business managers	Risk managers	Incident manager
Definition of maturity levels	++	Unknown[b]	++	−−	+	+

[a] - The model v1.3 is available for free, but the newest version (v2.0) is paid
[b] - As the model is paid, the maturity levels could not be reviewed in full

Security Incident Maturity Model - SIM3

The Security Incident Maturity Model or SIM3 is a maturity model that is concentrated on the response to security incidents (Stikvoort, 2010). This model is the most specialised model of the MCMs reviewed in this research. In the SIM3 model the readiness of an organisation to a security incident is measured. This is done on four aspects: organisation, human, tools and processes.

Within the four aspects mentioned above, there are multiple parameters that are looked into by the model. All of the four aspects deliver relevant parameters of this research, therefore none are left out.

3.2.3 Factors from maturity capability models

From the MCMs there were three decision-making factors that have been mentioned four times: use quantifiable measurements of the countermeasure, reduce a risk with the countermeasure, and fit countermeasure in the business context. These three factors are included in both the more abstract CMMI-DEV model (MCM1) and the more specific models for IS like ISMM and MMGRSeg (MCM4, MCM5). This shows that choosing countermeasures based on risks in a quantifiable way is of major importance. In addition the countermeasure should fit the business context of the organisation to be effective.

Allocating sufficient proper resources to security is also mentioned in the maturity models. Some focus on allocating enough resources, mostly on allocation enough people, (MCM2, MCM3) and MCM6 focuses mostly on the right resources by looking at the skillset of people. Taking the available resources into account therefore, is key in choosing the right countermeasure.

Table 3.6.: Factors found in maturity models

Factor	Reference
Use quantifiable measurements for evaluation of the countermeasure	MCM1, MCM3, MCM4, MCM5
Reduce a risk with the countermeasure	MCM1, MCM2, MCM3, MCM4
Fit countermeasure in the business context	MCM1, MCM2, MCM4, MCM5
Take the available resources into account (funding and knowledge)	MCM2, MCM3, MCM6
Choose countermeasures from best-practices	MCM1, MCM2, MCM6
Assign responsibility of the countermeasure	MM5
Get backing for the countermeasure	MM6

3.3 Factors from security consultants

Now that the exploration of decision-making factors about countermeasures in science is finished, an exploration in practice is done. With the third source of information in the exploration phase, the decision-making factors that are important to security consultants are identified. Security consultants have seen many organisations and thus know what factors are important to be able to choose the right countermeasures.

3.3.1 Methodology

To receive the information from the security consultants there are several possible ways such as via surveys, interviews, focus groups, observations and (data) extraction. Interviews can be used to gather background information with expert knowledge and a good description of processes (Harrell and Bradley, 2009). As the aim of the interview is to get a description of factors that influence the decision-making process about countermeasures, an interview is the appropriate method. Semi-structured interviews allow for deep-diving into a certain topic, fully allowing the respondent to express their story (Harrell and Bradley, 2009). Semi-structured interviews feel like more of a conversation, which helps respondents to open up more (Rabionet, 2011). Therefore, a semi-structured interview is used to collect information from security consultants.

The RAND National Defence Research Institution (Harrell and Bradley, 2009) provides a clear and complete overview of the steps that need to be taken to prepare and conduct a semi-structured interview. Table 3.7 describes the complete design of the interview.

3.3.2 Results

The interviews with 5 security consultants are conducted within a time-frame of just over a week. All consultants are working for the company this research was conducted at. The consultants have between three and ten years of experience in the field of risk management and IS. They all have had experience with risk management and advising about countermeasures. The transcriptions of the interviews can be found in Appendix D. The summary of the factors mentioned by the consultants during the interview can be found in Appendix D as well, in Table D.1 on page 123.

The security consultants share the same perspective on IS. This is reflected in the first factor they all mention as important to take into account when making decisions about countermeasures: reducing a risk with the measure. All of them stress the importance of using risk management as a basis on which organisations can build to choose the appropriate countermeasures. Two of the consultants (C2, C5) mention explicitly that there should be goal for a countermeasure and this is always a risk that is mitigated by this countermeasure. This is also referred to when discussing the ‘mistakes’ that organisations make. The biggest flaw is not using risks to choose a countermeasure. The shared opinion by all respondents

Table 3.7.: Design of exploratory interview with security consultants

Phase	Description
Framing the research	
Research question	What factors should be taken into account for the decision-making process about security countermeasures?
Source	Security Consultants
# respondents	5
Sampling	Convenience sample: *Available consultants in a fixed time period of one week are asked.*
Designing questions & probes	• What factors, do you think, are important to take into account when making decisions about which countermeasures to implement? • What are the biggest flaws of organisations when making these choices? • When, do you think, can organisations make well-justified decisions about countermeasures?
Developing the protocol	
Introduction	Security consultants are asked to participate in this research at the office
Ground rules	The interview... ... will take up 30 minutes. ... aims to explore the factors, not create one truth. ... will only be used within the context of the research. ... is strictly confidential. ... be recorded in notes. ... will be reported about in the master thesis, but will be anonymised to safeguard the privacy of the respondent.
Questions & probes	*See questions & probes above*
Closing	No follow-up required
Preparing for the interview	No specific preparation required
Conducting the interview	The interview guide as described by the protocol will be followed
Capturing the data	Afterwards, the interview will be (partly) transcribed

therefore is that taking countermeasures needs to be based on a risk analysis so that the countermeasure serves a purpose in securing the organisation.

Funding and resources for implementing countermeasures are essential for the success of implementing countermeasures, according to all respondents. The organisation should

allocate time (and people) to implementing the countermeasure as well as the money to buy a certain product or service. When organisations do not think through what a countermeasure brings to the organisation (e.g. monitoring the infrastructure costs 1 full time employee extra), a countermeasure could fail completely. In addition to the amount resources that the organisation allocates to implementing countermeasures, the knowledge that is available in-house is vital. All of the security consultants interviewed stressed that the knowledge that people in the organisation have is of major importance. The knowledge in-house is important to be able to identify the different options there are for countermeasures (C2, C3, C4, C5). People that have extensive knowledge about the possibilities available to mitigate a risk, are more able to come up with the best countermeasure. Furthermore, the knowledge in house helps to implement the countermeasure well (C1, C2). If there is no knowledge available to implement the countermeasure well, the measure will be more likely to be ineffective. Therefore, taking into account the resources necessary for the countermeasure is important.

Table 3.8.: Factors mentioned by security consultants

Factor	Reference
Reduce a risk with the countermeasure	C1, C2, C3, C4, C5
Take the available resources into account (funding and knowledge)	C1, C2, C3, C4, C5
Get backing for the countermeasure	C1, C2, C3, C4, C5
Choose countermeasures from best-practices	C4, C5
Fit countermeasure in business context	C2, C4

3.4 Summary of exploration

This chapter describes the exploration phase of the design of the capability model to assess the decision-making process about countermeasures. The core research question of this chapter is SQ2: '*What factors should be taken into account for the decision-making process about security countermeasures?*'.

Three kind of sources - literature, existing maturity capability models, and security consultants - have been researched to get an overview of the factors that are relevant to take into account when making a decision about countermeasures. In total 27 sources are studied.

The result is a list of 8 decision-making factors. The factors found are presented in Table 3.9 with the weighted percentage of sources that discuss them. Each kind of source has equal weight in the percentage of the sources that mentions the factor. Table 3.10 presents the factors with the source that has taken into account that factor. In Appendices B, C and D a more detailed examination of the factors can be found.

Most sources stress the fact that countermeasures that an organisation takes should reduce an identified risks. In particular this is emphasised by the security consultants who also see *not* basing countermeasures on risks as the biggest flaw at making decisions about countermeasures that need to be implemented. Risk management is the basis for choosing countermeasures. Only when a countermeasures reduces a risk, the measure has a defined goal.

Table 3.9.: Factors referred to by % of reviewed sources

Factor	% literature	% maturity models	% security consultants
Reduce a risk with the countermeasure	50%	67%	100%
Take available resources into account (funding and knowledge)	50%	50%	100%
Fit countermeasure in the business context	69%	67%	40%
Get backing for the countermeasure	69%	17%	100%
Choose countermeasures from best-practices	56%	50%	40%
Use quantifiable measurements for evaluation of the countermeasure	69%	67%	-
Assign responsibility of the countermeasure	38%	17%	-
Choose countermeasures that prevent previous incidents	25%	-	-

Table 3.10.: Summary of all factors found in exploration

Factor	Literature	Maturity models	Security consultants
Reduce a risk with the countermeasure	L01, L03, L07, L09, L11, L12, L16, L17	MCM1, MCM2, MCM3, MCM4	C1, C2, C3, C4, C5
Take available resources into account (funding and knowledge)	L01, L02, L09, L10, L12, L17, L18, L19	MCM2, MCM3, MCM6	C1, C2, C3, C4, C5
Fit countermeasure in the business context	L01, L02, L05, L07, L09, L11, L12, L14, L15, L17, L19	MCM1, MCM2, MCM4, MCM5	C2, C4
Get backing for the countermeasure	L01, L03, L05, L09, L11, L12, L14, L15, L17, L18, L19	MCM6	C1, C2, C3, C4, C5
Choose countermeasures from best-practices	L01, L07, L09, L10, L12, L14, L15, L16, L17	MCM1, MCM2, MCM6	C4, C5
Use quantifiable measurements for evaluation of the countermeasure	L01, L03, L04, L07, L09, L10, L11, L12, L15, L16, L17	MCM1, MCM3, MCM4, MCM5	-
Assign responsibility of the countermeasure	L03, L05, L11, L12, L14, L19	MCM5	-
Choose countermeasures that prevent previous incidents	L03, L12, L15, L18	-	-

Scientific literature and maturity capability models both speak of the use of quantified measurements for the choice of countermeasures in IS. However, this is not discussed by the security consultants. The gap between science and practices is shown in this factor. As discussed before, scholars mention using quantified measurements as a relevant factor, but it takes time and effort to actually use the measurements in practice.

Surprisingly, lessons learned from previous incidents or from previous experiences is only mentioned in literature. Maturity capability models and security consultants do not mention that the countermeasure should prevent previous incidents from happening again. However, consultants will probably implicitly take the history of the organisation into account. All security consultants do mention the context of the organisation in some way to be relevant to decision-making about countermeasures.

3.5 Implications

Going forward, the eight decision-making factors about countermeasures that are identified are used as the basis to create the capability model. The factors are input for the Delphi study conducted and reported in Chapter 4.

In this chapter these eight decision-making factors are found from multiple methods from multiple sources. As indicated by Seddon and Scheepers (2012), when a number of studies claim that X causes Y, it becomes likely that X indeed does lead to Y. The decision-making factors about countermeasures found are described as factors that do cause better information security. Therefore, the claim of this research is that the factors found do improve decision-making about security countermeasures. The claim about the improvement of decision-making by taking into account these factors holds whenever the context is information security. It is likely the claim is stronger when the context is risk management.

However, the factors identified from literature, maturity capability models and security consultants is not the only addition to this research from the exploration phase. A lot of knowledge has been gathered about previous research and the structure of already existing maturity capability models. The decision-making factors that are excluded are of major importance in the next steps as they could be of importance again in the Delphi study. The reasoning of not including the factors is vital in order to decide about the factors that are included in the capability model of this research.

Furthermore, by reviewing a number of existing maturity capability models, ideas about effective structures of those models are obtained. Especially, the CMMI-model (CMMI Product Team, 2010) and the C2M2-model (Christopher et al., 2014) have provided valuable insights to this research. The structure of CMMI has been used by a number of different maturity models and is tested and proven in practice. The C2M2-model provides a structure in which certain factors are assessed by indicators. This structure is close to what is required of the capability model of this research as well.

Decision-making factors from practice

4

> *Sometimes when you innovate, you make mistakes. It is best to admit them quickly, and get on with improving your other innovations.*
>
> **— Steve Jobs**
> (Former CEO of Apple Inc.)

To create the capability model about the decision-making process about security countermeasures, both scientific sources and sources from practice are reviewed. The previous chapter looked mostly into scientific sources in order to provide a list with relevant decision-making factors. This chapter adds to this with testing these factors in practice by conducting a Delphi study.

This chapter tackles three sub-questions of this research. First, the decision-making factors are reviewed by the industry experts to answer '*What factors should be taken into account for the decision-making process about security countermeasures?*'. Then, to answer '*How can be determined to what extent a factor, is present in the decision-making process?*', indicators are identified for each of the decision-making factors. Answers to both of these questions contribute to creating the capability model to answer the last sub-question *'How can the capability level of the decision-making process about security countermeasures be determined using the created model?*'.

A Delphi study is carried out in order to base the capability model on experience from practice. The methodology of the Delphi study is described in section 4.1. Then, in section 4.2, the results of the first round of the Delphi study are presented. The section afterwards, section 4.3, describes the results of the second round of the Delphi-study and section 4.4 presents the third and final Delphi round. Section 4.5 shows the implications of the Delphi study for this research.

4.1 Methodology

According to Linstone and Turoff (1975) "*Delphi may be characterised as a method for structuring a group communication process so that the process is effective in allowing a group of individuals, as a whole, to deal with a complex problem.*". The Delphi method has four features: (1) anonymity, (2) iteration, (3) controlled feedback, and (4) statistical aggregation of group

response (Rowe and Wright, 1999). Making a decision is complex by definition and it does not lend itself for precise analytical techniques, but it can benefit from subjective judgements. Therefore, this research employs a wide range of people from practice to create a capability model about making decisions about security countermeasures. For this reason and reasons of different backgrounds of the participants to the study, which also makes frequent group meetings infeasible, a Delphi study is the appropriate method (Linstone and Turoff, 1975). This approach fits well with the creation of a maturity capability model as exemplified by a number of maturity capability models creation studies (De Bruin and Rosemann, 2005; Mettler, 2011; Smits and Van Hillegersberg, 2015; Van Dijk, 2017; Vermeij, 2018). Thus, a Delphi study is used to collect data from practice.

The objective of the Delphi study is to develop a technique to obtain most reliable consensus of a group of experts by a series of questionnaires with controlled opinion feedback (Dalkey and Helmer, 1963). In this research the typical Delphi process as presented by Skulmoski et al. (2007) will be used, also in a three round Delphi process. The process that is followed in this research is presented in Figure 4.1.

4.1.1 Delphi study design

This Delphi study consists of three rounds. Rowe and Wright (1999) states that the accuracy tends to increase over the Delphi rounds and therefore a greater number of rounds will be more accurate. This study is limited to three rounds because of time constraints. The focus in the first round is to verify the factors found from the exploration phase and to add to this with factors that are deemed critical by the industry experts or *panellists*. In the second round the renewed list of factors is tested on their relevance and indicators for each factor are discussed. In the last round, the full capability model is presented to the panellists and is put up for evaluation. Table 4.1 presents an overview of these rounds.

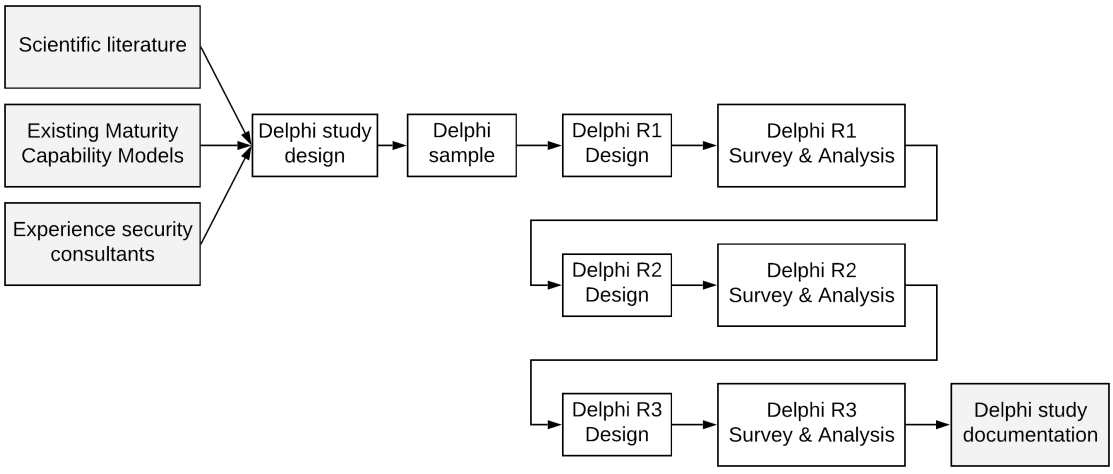


Figure 4.1.: Three-round Delphi methodology

Table 4.1.: Study design for Delphi study

Preparation	*Survey to panellists*
Round 1 • Produce initial list of important decision-making factors • Define the decision-making factors	
	Round 1 • Rate the importance of factors found • Add relevant other factors • Brainstorm on indicators on decision-making factors
Round 2 • Revise list of relevant factors • Propose list of indicators for every factor	
	Round 2 • Rate the importance of revised list of factors • Rate the relevance of the indicators
Round 3 • Create final list of factors and indicators • Produce complete capability model	
	Round 3 • Evaluate capability model • Propose possible improvements to the model

4.1.2 Delphi study sample

Selecting the research sample is a vital component of the Delphi study, as it is the sample that determines what opinions are included in the research (Okoli and Pawlowski, 2004). According to Skulmoski et al. (2007) there are four requirements for 'expertise' in the Delphi study: (1) knowledge and experience with the issues under investigation; (2) capacity and willingness to participate; (3) sufficient time to participate; and, (4) effective communication skills. With these requirements in mind the sample can be created.

Selecting panellists, the experts on the subject, is a step-by-step process (Okoli and Pawlowski, 2004). First is identified what relevant disciplines, skills and organisations should be contacted. For this research the Delphi study is focused on people from practice as this is the biggest unknown in this area. Everyone who has ever participated in making a decision about countermeasures in IS can be a relevant source of information to this research. These people all have their own opinions on what is important to take into account when making a decision

on countermeasures. There is no limit to on what level of decision-making the panellist is involved, the different views can complement each other.

The second step is collecting names of possible panellists. This is be done based on the evaluation of security consultants of the company that is involved in the project. Their evaluation is based on the requirements mentioned before, especially on their expertise and the willingness and time needed. The consultants provide the research with names of those people who are expert in the area and are possibly willing to participate.

The third step is to invite the panellists. This is done by an invitation via email with a letter that explains more about the project. The invitation is sent to over 120 people in different organisations. Following recommendations from Okoli and Pawlowski (2004) a preferred sample is between 10 and 18 panellists. In the end, this has resulted in 12 panellists for the first round of the Delphi-study. Their demography can be found in Tables 4.2 and 4.3.

Table 4.2.: Sector of participants

Sector	#
IT	3
Education	2
Manufacturing	2
Financial services	1
Media	1
Managed security services	1
Publisher	1
Health care	1
	12

Table 4.3.: Role of participants

Role	#
Security officer	5
CISO	2
CTO	2
IT security manager	2
CQO	1
	12

4.2 Delphi round 1

The first round of this Delphi study is aimed at evaluating the decision-making factors about countermeasures found in the exploration. The Delphi study aims to add to this with any factors that are not brought up by literature, maturity models or security consultants. Secondly, indicators for each of the decision-making factors are asked to the panellists.

The first survey is filled in by 12 panellists. More detailed information on the first round of the Delphi study can be found in Appendix E, including the complete survey in Appendix E.1.

4.2.1 Evaluation of factors found in exploration

The first part of Delphi round 1 is fully about rating the relevance of the factors found in the exploration phase. Panellists are asked to score each factor with *strongly disagree* (score 0), *disagree* (score 1), *neutral* (score 2), *agree* (score 3) or *strongly agree* (score 4). Figure 4.2 presents the average and spread for each of the factors as indicated by the panellists.

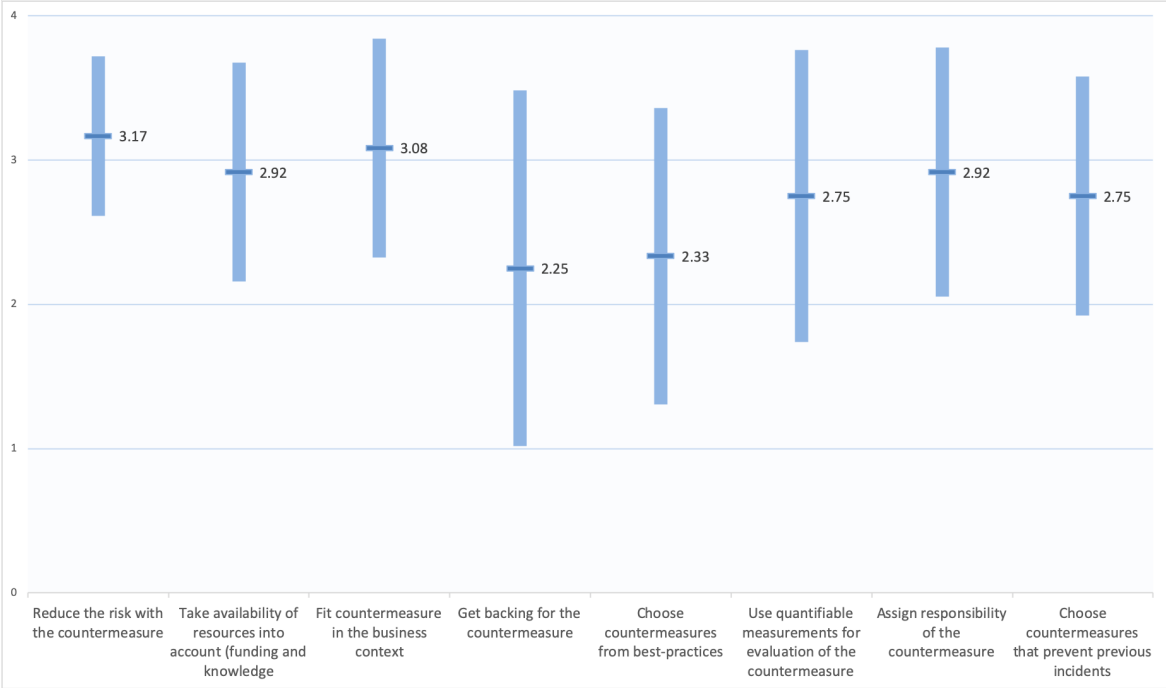


Figure 4.2.: Results of decision-making factors

As can be concluded from Figure 4.2, all of the decision-making factors about countermeasures are found (slightly) relevant by the panellists. Every factor scores more than 2 (*neutral*) on average and which means that for all factors the panellists are leaning towards '*agree*'. The most important factors according to the panellists are the risks and business context. Both of those factors score above 3, which indicates that on average panellists agree with the relevance of those factors.

One overall finding is that panellists have responded to the decision-making factors as if every factor is of major importance to all decisions. However, in reality each factor can bring a relevant insight to the table in order to make the most effective and cost-efficient decision. This could differ from countermeasure to countermeasure and from organisation to organisation. The aim in this model is not to state that all of these factors are fully integrated in the decision-making process, but more to provide quality to the process.

Get backing for the countermeasure

The factor '*Get backing for the countermeasure*' scores lowest. More in depth investigation on the answers shows that a number of panellists indicate that some measures do not need backing in the organisation as these measures just need to be taken (e.g. measures to ensure compliance). Others indicate that there is no need for backing at the employee-level, as the top management can simply direct that the employees need to comply with the countermeasure as set by top management. In contrast, there are also panellists who strongly agree with the factor, hence the high spread for this factor. On examination of the answers about this factor, it is evident that the definition of the factor was not clear and that panellists have interpreted it differently. Therefore, going forward the factor is not neglected, but the definition is changed to better suit the purpose of the factor.

Choose countermeasure from best-practices

Best-practices scores second lowest. In addition to the low average score, the spread is also fairly high. Investigation into the reasons for this score reveals that a number of panellists think that best-practices are not relevant for all (in particular small) organisations. The best-practices should only be considered when it suits the organisation. When it does suit the organisation, it can provide effective and cost-efficient countermeasures. The description of the factor '*Choose countermeasure from best-practices*' is changed to better reflect this.

Integration into other factors

Two of the decision-making factors '*Take availability of resources into account*' and '*Assign responsibility of the countermeasure*' are found reasonably important by the panellists with just below *agree*. These factors are therefore included in the 0.5 version of the model. Upon creating the 0.5 version, it became evident that these factors are important throughout the model and not just as two separate factors. Therefore, these factors are integrated into the other factors by using it as a practice at the second and third factor indicator level (see Chapter 5 for more on this).

Additional factors

Panellists are provided with the opportunity to add factors to the list that they deemed important and not yet present. The complete list of their answers can be found in Appendix E.2.

Of the additional factors provided in the survey, 35% of the answers is about compliance to laws, regulations or third-party contracts. This factor was not yet present in the list of factors derived in the exploration of this research. As this factor is most mentioned by the panellists, the factor is added to the list of relevant factors.

Another change in the list of factors is the addition of awareness of the countermeasure. Although awareness was excluded in the exploration, multiple panellists have indicated something about awareness in different locations. The awareness in the organisation about the need for and the relevance of the countermeasure, determines the effectiveness of the countermeasure. Without awareness on security, the countermeasure will most likely be not as effective as it could be. Awareness about the need for the countermeasure is therefore added to the list of decision-making factors about countermeasures.

4.2.2 Indicators of decision-making factors

The second part of the survey in the first round of the Delphi study is about the indicators that show that the the presence of the factor in the organisation. The complete list of answers provided by the panellists is shown in Appendix E.2.

The indicators mentioned by the panellists for each of the factors are reviewed and used to create the factor indicator levels for the 0.5 version of the model. The existence of each of the factors in the decision-making process about countermeasures can be proved by one or more of the indicators mentioned. As this is the first time these indicators are collected and mentioned, there is no evaluation of these indicators. This will be tested in the second round of the Delphi study.

4.2.3 Model v0.5

In this first round of the Delphi study preliminary answers are given to two of the research questions. The decision-making factors about countermeasures are researched in practice in order to get a complete list of relevant factors. Furthermore, the indicators to show the presence of the factor in the decision-making process are explored.

Resulting from the first round of the Delphi study the first version of the model is created. As described above, two factors (resources and responsibilities) are integrated into the other factors and two other factors (compliance to rules and regulations & awareness about the countermeasure) is added to the list. Consequently, the total list of maturity factors consists of 8 factors.

A provisional division is made in order to create more structure in the entire model. The eight factors are divided into three domains: business, bytes and behaviour. Other maturity capability models also have divided the factors into domains to provide necessary structure. The division in this model is equivalent to the division of the SOC-CMM model (Van Os, 2016), which uses business, people, processes, technology and services. In overview the 0.5 version of the model looks like Figure 4.3.

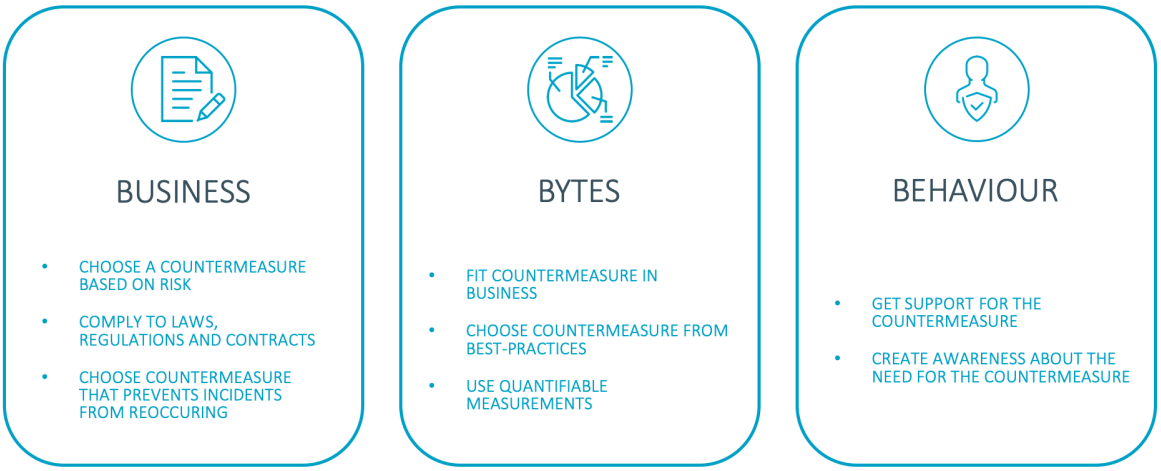


Figure 4.3.: Model version 0.5

4.3 Delphi round 2

The second round in the Delphi study assesses the 0.5 version of the model. In this survey the renewed decision-making factors about countermeasures are reviewed by the panellists and the different factor indicator levels for each of the factors are analyzed. The complete survey can be found in Appendix F.

The survey has been sent to the 12 panellists that have participated in the previous round and it was open for two weeks in which they are reminded twice. This has resulted in 8 responses, of which one of the panellists did not complete the entire survey. Some of the panellists responded that they had a lack of time or had difficulties with the language and were therefore excluded from the following surveys.

Due to an error in this survey one of the factors, '*Fit countermeasure in business*', was not included in two of the questions. This error has been corrected as soon as it came to light (within 24 hours). Unfortunately, four out of the eight panellists already had filled in the survey by then.

4.3.1 Evaluation of renewed factors

Firstly, the renewed factors are discussed with the panellists. Resulting from the first survey, two factors have been integrated in the others and two factors are added. Additionally, all of the descriptions for the factors have been changed to better describe the decision-making factor. The panellists are asked whether they now would include (score 2) or exclude (score 0) the factor, or are neutral (score 1) towards it. The results are shown in Figure 4.4 and Table 4.4.

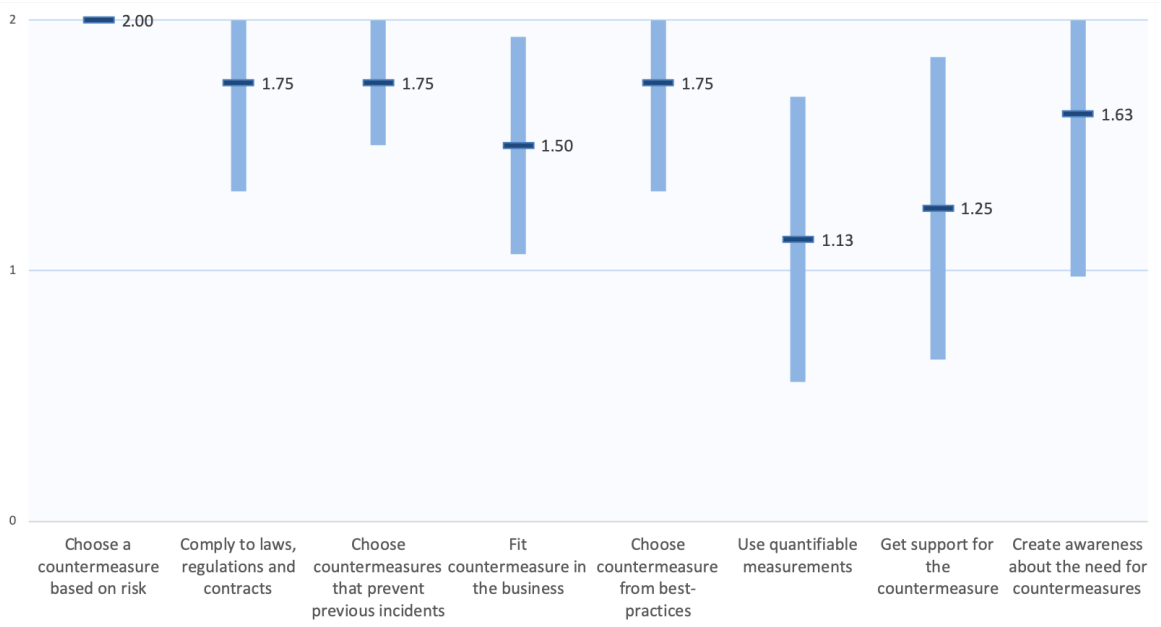


Figure 4.4.: Evaluation of renewed factors

Overall, all panellists agreed on the inclusion of most factors. The average of all factors is above '*neutral*' and most of the factors lean towards '*include*'. This is also reflected in the low spread of the factors. Two of the decision-making factors do not need discussion. Both '*Choose countermeasure that prevents previous incidents*' and '*Choose countermeasure from best-practices*' are broadly accepted by the panellists and should be included.

Choose a countermeasure based on risk

According to all the panellists choosing a countermeasure based on risk is very important when making a decision about a countermeasure. This is reflected in the unanimous inclusion of this factor.

Comply to laws, regulations and contracts

Compliance has been added to the model in reaction to the feedback in the first round of the Delphi study. This has been received well by the panellists with an overall *inclusion* of the factor. Therefore, this factor will remain included in the model.

Fit countermeasure in business

Due to an error in the survey of the second round of the Delphi study, this factor has been judged by only half of the panellists. Nonetheless, they indicated that this decision-making factor should be included in the model. The fit in the business determines the effectiveness of the security countermeasure according to them.

Use quantifiable measurements

This decision-making factor has the lowest average score, with a score almost '*neutral*'. The spread on this factor is relatively high too. This shows that using quantifiable measurements is not something that all panellists believe to be beneficial for making a good decision about countermeasures. From the first and second round of the Delphi study has become apparent that there are two sides of using quantifiable measurements. Most panellists do think that quantified measurements can improve the decision-making, but they see difficulties in practice. It is difficult to put numbers to the countermeasure as they are sometimes simply not available. For the sake of pragmatism, quantification measurements are therefore neglected.

Although panellists see obstacles using quantifiable measurements, literature has shown the value of quantification on the quality of the decision. The issues of the panellists mostly have to do with time constraints or availability of data. These arguments are not valid for making a quality decision about countermeasures. Thus, the factor is not excluded from the model.

Get support for the countermeasure

The second lowest score is for the factor '*Get support for the countermeasure*'. Again, the spread of this factor is relatively high as well. From the first and second round, the feedback has been on the way that top management is behind the countermeasure is key. One of the panellist even states that it is *in or out*: if you do not obey company rules there is no place for you.

For the third round of the Delphi study, the description has been changed more towards the backing of top management. In order to reflect this even better, the description and the factor indicator levels are changed. The factor is not excluded as a large number of panellists do agree with including the decision-making factor and literature indicates that commitment of the organisation is important to make the organisation secure.

Create awareness about the need for countermeasures

Resulting from the first round of the Delphi study, this factor has been added. Most panellists seem to agree with the inclusion of this factor in the model. However, the spread of this factor is the highest spread reported in this questions. There is no clear explanation to the high spread, other than that some panellists want to include and some wont to exclude this factor.

From the feedback given on the factor indicator levels of this factor, the description and the factor indicator levels of this factor are changed slightly. As the average of creating awareness of about the need for the countermeasure is above 1,5, the overall consensus is to include the factor in the model.

4.3.2 Factor Indicator Levels

The second part of the second round of the Delphi study is about the Factor Indicator Levels (FILs). Panellists are asked whether they agree with the definition as given or would change some of the FILs.

Table 4.4.: Changes to Factor Indicator Levels

Factor	Changed
Choose a countermeasure based on risk	FIL1, FIL2
Comply to laws, regulations and contracts	FIL2, FIL3
Choose countermeasure that prevents previous incidents	FIL3
Fit countermeasure in business	*Nothing*
Choose countermeasure from best-practices	*Nothing*
Use quantifiable measurements	FIL2, FIL3
Get support for the countermeasure	FIL1, FIL3
Create awareness about the need for countermeasure	FIL1, FIL2, FIL3

Most of the FILs needed minor changes because of the feedback of the panellists. However, two of the factors were already perfect according to the results in the survey. Table 4.4 shows for what factor the levels have been changed due to the feedback.

4.3.3 Structuring the model

In order to provide structure in the model, a division has been made into three domains: business, bytes and behaviour. The panellists are asked to assign each of the decision-making factors to the domain that they think fits best. The result is presented in Figure 4.5. A score of 0 implies that the factor should be in the domain *business*, score 1 is the domain *bytes* and a score of 2 is the domain *behaviour*.

Of all decision-making factors about countermeasures, of just one factor it is not entirely clear into what domain it should be placed. The awareness about the need for the countermeasure has an average of 1,43 and is therefore closest to the domain *bytes*. However, none of the panellists have chosen to place *awareness* in the *bytes*-domain. Most panellists think it should be in the domain *behaviour* (score 2) and some think it should be in *business* (score 0). Because of this, the factor is placed in the *behaviour*-domain.

The decision-making factors about countermeasures are grouped into the domains as follows:

Business

- Choose a countermeasure based on risk
- Comply to laws, regulations and contracts
- Fit countermeasure in business

Bytes

- Choose countermeasure that prevents previous incidents
- Choose countermeasure from best-practices
- Use quantifiable measurements

Behaviour

- Get support for the countermeasure
- Create awareness about the need for the countermeasure

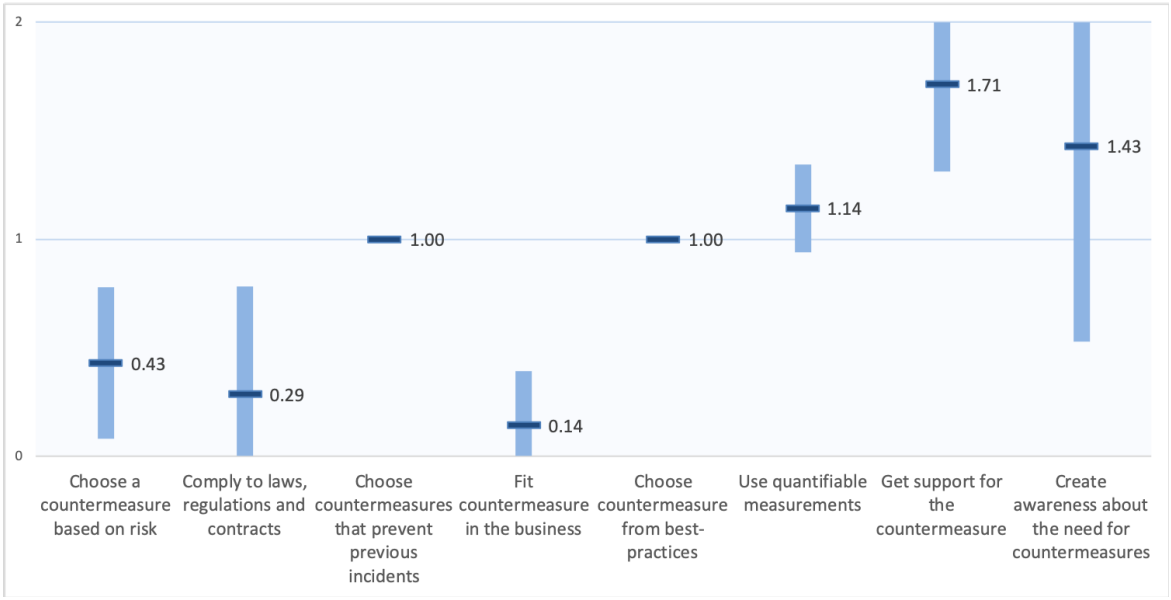


Figure 4.5.: Division of factors in domains

4.3.4 Model v1.0

The second round of the Delphi study has answered the research question '*What factors should be taken into account for the decision-making process about security countermeasures?*'. There are eight decision-making factors that need to be included in the model. Additionally, the indicators for these factors have gotten feedback in this round.

Feedback on the decision-making factors and the complete model is given in the second round. The complete model has been challenged in practice and is adjusted according to the feedback received. This has resulted in the version 1.0 of the model which is presented in Chapter 5, see also Figure 4.6.

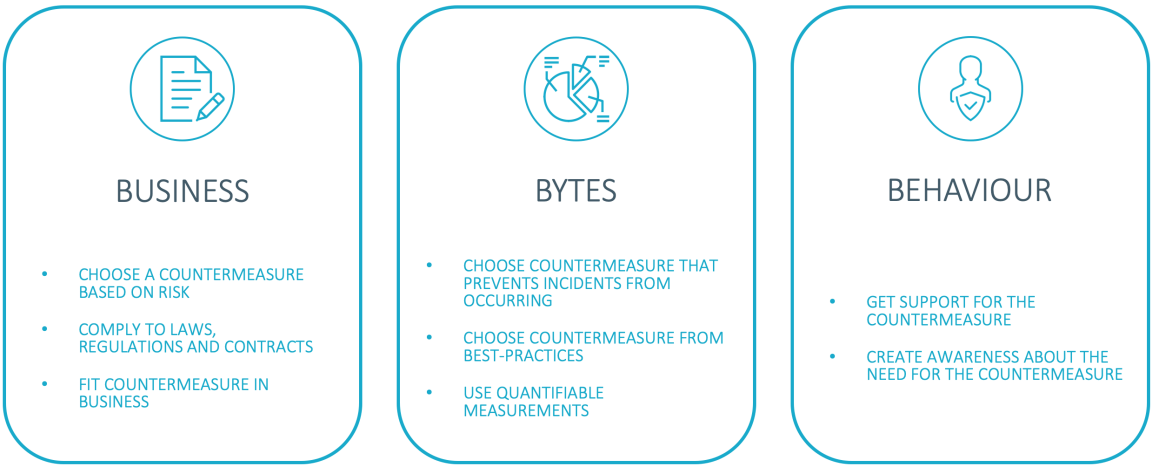


Figure 4.6.: Model version 1.0

4.4 Delphi round 3

The third round of the Delphi study has the aim to evaluate the version 1.0 of the Decision-Making Capability Model for Security Countermeasures (DMCMSC). In this third survey the panellists are asked to evaluate the decision-making factors and their factor indicator levels. In addition the most important factors are identified and the use of the model is discussed. The survey has been filled in by 8 out of 10 still involved panellists. One of them did not complete the entire survey. The full survey can be found in Appendix G.

In addition to the panellists from practice, the consultants who have been interviewed in the exploration phase (see Section 3.3) have also been asked to participate in the evaluation. Four out of the five consultants did participate and provided additional and relevant insights.

4.4.1 Evaluation of Factor Indicator Levels

The first part of the third round evaluates the Factor Indicator Levels (FILs) as they are composed as version 1.0 of the DMCMSC. These definitions can be found in Chapter 5. The panellists are asked whether they *strongly disagree* (score 0), *disagree* (score 1), *neutral* (score 2), *agree* (score 3) or *strongly agree* (score 4) with the definition. This evaluation is done by both the panellists from practice and the consultants and thus this has been filled in by 12 people in total. A summary of the results of this part can be found in Figure 4.7 and can be found in more detail in Appendix G.

In general, the respondents agree with all of the definitions. All of the decision-making factors score higher than *neutral*, which indicates that every definition is broadly accepted. The spread on each of the FILs is below 1 (except for '*Choose countermeasure based on best-practices*') and this proves that a consensus is practically reached. Closer examination reveals that the spread can mostly be explained by the difference between '*agree*' and '*strongly agree*'. Whenever there was disagreement, this was in all cases because of one (not necessarily the same) panellist.

Highly approved decision-making factors

For three of the factors, none of the panellists disagreed with the definition. This goes for '*Choose a countermeasure based on risk*', '*Comply to laws, regulations and contracts*' and '*Get support for the countermeasure*'. For these factors both the average score is high - above 3 which indicates more than 'agreed' - and the spread is low, this shows that all panellists were in agreement with each other. There were a few small comments on the factors for improvements of FILs, mostly language related.

Fit countermeasure in the business

For this factor one of the panellists disagreed with the definition and one other was '*neutral*' towards it. Two of the panellists explained their score by indicating that they did not fully agree with FIL3 of this factor. One of them commented that a practice should be added that shows that the organisation thinks about ways that the countermeasure blocks the way-of-working. The other panellists explained that sometimes extra work or steps cannot be minimised as you just have to comply. These were reasons for them to score lower than '*agree*' whereas all other scored *agree* or *strongly agree*.

Choose countermeasure that prevents incidents from occurring

Although the average on this factor is above *agree*, there is a bit of disagreement among the panellists. Particularly one of the panellists scored this factor lower, as he explained that in his opinion there is a lack of focus on preventing incidents. He thinks that this factor is too much focused on incident management rather then the prevention of incidents.

Choose countermeasure from best-practices

This factor presents the highest spread. This spread can completely be explained by the '*strongly disagree*' score of one of the panellists. He is the only panellist that does not score an '*agree*' or '*strongly agree*' on this factor. He comments on his score that best-practices are a necessity and that there is no way around it. In contrast, he thinks that documenting everything as the practices in the FILs state are totally unnecessary.

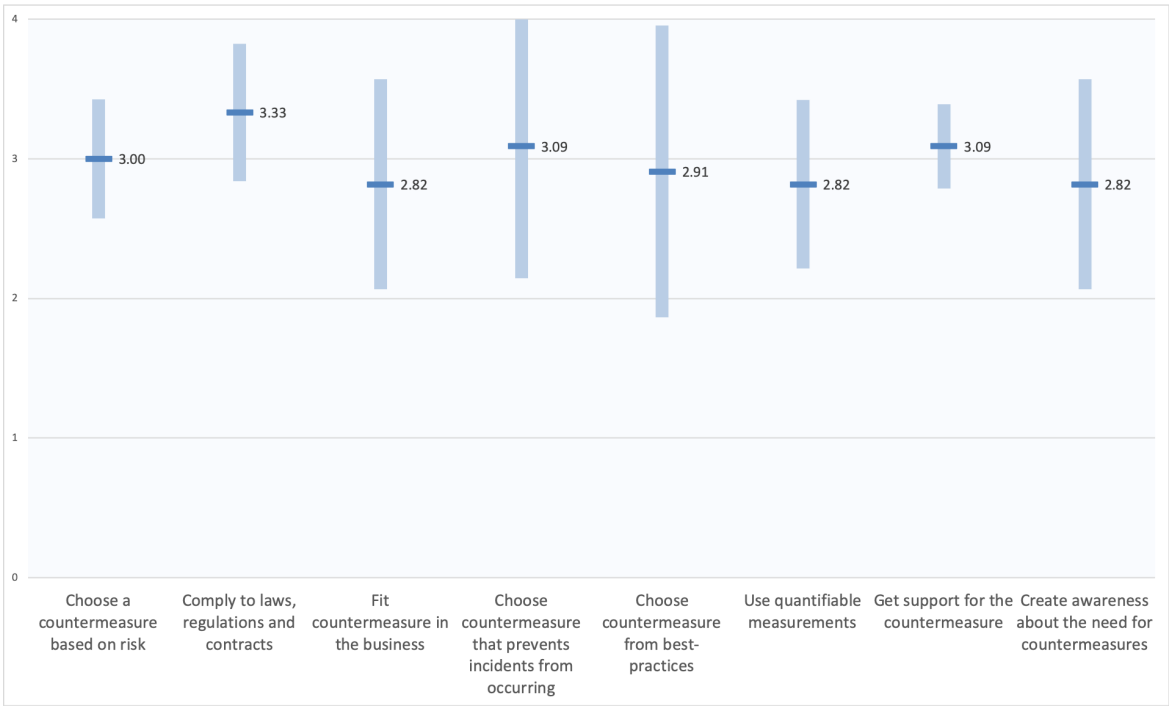


Figure 4.7.: Evaluation of Factor Indicator Level per factor

Use quantifiable measurements

Ten out of eleven panellists that answered this question, scored '*agree*' for this factor. The last panellist disagreed with the factor as not everything can be quantified in his opinion and he mentioned the reputation of an organisation as an example. In his comment, he explained that he thinks that quantifying is relevant, but it is often not a necessity as the gut feeling can produce the same results.

Create awareness about the need for the countermeasure

Two of the panellist made a comment on this factor, of which one was in disagreement with the definition. Both comments were about a different way of showing awareness of in the organisation. One of the panellists focused more on the awareness of top management. The other explained how his organisation classifies the different levels of awareness. In order to be more relevant to him, this factor should be changed more towards their view on awareness.

4.4.2 Most important decision-making factors

In the second part of the third survey, the panellists (only those from practice) are asked to score their top 3 of most important decision-making factors about countermeasures. The seven panellists each indicated their top 3 and that gave the results as presented in Table 4.5. The lowest score is the closest to position 1 and this builds up to position 4 (as there is no position 5-8 available in the survey).

The most important factor according to the panellists is '*Choose a countermeasure based on risk*', closely followed by '*Comply to laws, regulation and contracts*'. This shows that having a solid basis to choose countermeasures is very important to the panellists; there has to be a reason to choose a countermeasure.

On the bottom the factor '*Use quantifiable measurements*' is chosen by none of the panellists in their top 3. Apparently, panellists do not see real value in putting numbers to their choice. It can, however, not be stated that it is not important, as the panellists in previous rounds of the Delphi study indicated that quantifiable measurements should be part of this model.

Table 4.5.: Most important factors according to panellists

	Factor	Avg. position
1	Choose a countermeasure based on risk	2,29
2	Comply to laws, regulation and contracts	2,43
3	Create awareness about the countermeasures	3,00
4	Fit countermeasures in business	3,14
5	Choose countermeasure from best-practices	3,57
6	Get support for the countermeasure	3,71
7	Choose countermeasure that prevents incidents from occurring	3,86
8	Use quantifiable measurements	4,00

4.4.3 Using the Decision-Making Capability Model for Security Countermeasures

The third and final part of this third round in the Delphi study is on the use of the model. The panellists are asked in what way they would be likely to use the model and to what end. They could answer in four ways: '*Very unlikely*' (score 0), '*Unlikely*' (score 1), '*Likely*' (score 2) and '*Very likely*' (score 3). Figure 4.8 presents the answers of the panellists.

For the panellists it is most likely that they would use the model for self-evaluating the decision-making process of their organisation. The main reason for the use would be to check which practices the model presents in order to improve the quality of decision-making in the organisation. Also the using the model to improve the quality of the decision-making process in the organisation is rather likely. On the other hand of the spectrum, it is very unlikely that the panellists would ask a third-party to use the model to assess their organisation.

Parts		Average	Spread
... check whether my organization is capable of making good decisions about countermeasures		1.7	0.7
... improve the quality of decision-making about countermeasures in my organization.		1.9	0.3
... let a third-party evaluate the capability of my organization about choosing countermeasures.		1.0	0.5
... self-evaluate the decision-making process of my organization.		2.6	0.5
... check which practices the model presents in order to improve the quality of decision-making in my organization.		2.0	0.5
... set up a decision-making process about countermeasures (when no process is present).		1.6	0.9
	1 2	**1.8**	**0.8**

Figure 4.8.: Usage of the Decision-Making Capability Model for Countermeasures

4.5 Implications

In this chapter a Delphi study over three rounds has been carried out. In the first and second round the research question '*What factors should be taken into account for the decision-making process about security countermeasures?*' has been answered. There are eight decision-making factors about countermeasures that need to be taken into account:

Business

- Choose a countermeasure based on risk
- Comply to laws, regulations and contracts
- Fit countermeasure in business

Bytes

- Choose countermeasure that prevents previous incidents
- Choose countermeasure from best-practices
- Use quantifiable measurements

Behaviour

- Get support for the countermeasure
- Create awareness about the need for the countermeasure

In the second and third round the research question '*How can be determined to what extent a factor, is present in the decision-making process?*' solved. Each of the decision-making factors have one or more indicators that show the presence of the factor in the decision-making process.

Lastly, the third round of the Delphi study the capability model is tested to provide an early answer to the question '*How can the capability level of the decision-making process about security countermeasures be determined using the created model?*'. Overall this showed that the Decision-Making Capability Model for Security Countermeasures would be used by decision-makers to self-assess their decision-making process in order to improve the quality of their process.

This Delphi study has shown which decision-making factors about security countermeasures are relevant to people from practice. The sample of panellists consists of all kinds of different organisations and a few different layers from the organisation (e.g. IT security vs. CISO). This has resulted in a sample which represents security decision-makers in the Netherlands. Consequently, the Decision-Making Capability Model for Security Countermeasures should be a good fit for organisations in the Netherlands that deal with security decisions. Decision-making on other aspects than information security countermeasures and in other countries can be different. Therefore, the Decision-Making Capability Model for Security Countermeasures could be unsuited for use there.

5 The Decision-Making Capability Model for Countermeasures

> *You can distill deterrence down to two factors: capability and will.*
>
> — **Chris Gibson**
> (Politician)

This chapter defines the Decision-Making Capability Model for Security Countermeasures (DMCMSC). The capability model is created by combining insights from science in Chapter 3 and practice in Chapter 4.

The Decision-Making Capability Model for Security Countermeasures focuses on providing quality in decision-making about countermeasures. In order to structure the DMCMSC, it adopts elements of the C2M2-model (Christopher et al., 2014) and the CMMI-model (CMMI Product Team, 2010). The model consists of three domains: *business*, *bytes* and *behaviour*.

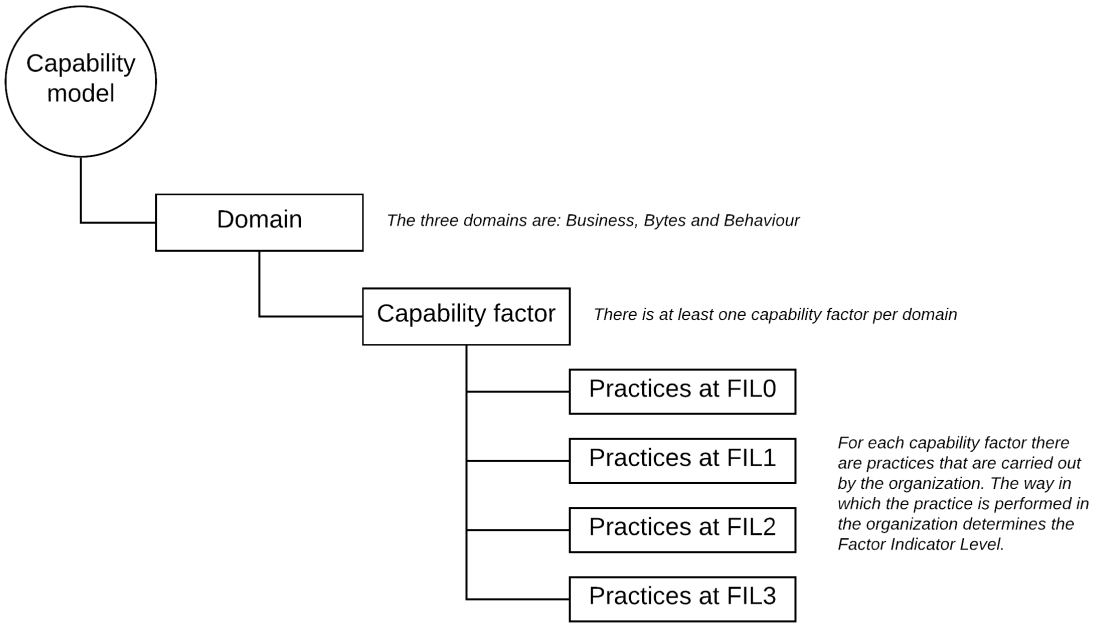


Figure 5.1.: Schematic overview of the capability model

Each domain entails a number of capability factors that determine the capability level of that domain. These factors are measured by a number of key indicators in four Factor Indicator Levels (FILs). Each level entails certain key practices are performed within an organisation in order to reach that level. A schematic overview of the model is presented in Figure 5.1.

The rest of this chapter is structured as follows. First, the domains of the DMCMSC are described in section 5.1. Afterwards the factor indicator levels are explained in section 5.2. The practices that are affiliated in the different levels are introduced and explained. The last section, section 5.3, defines the full capability model with the different factors per domain and the factor indicator levels for each factor.

5.1 Domains

The model consists of three domains: business, bytes and behaviour. The domains describe all aspects of IS and therefore also the aspects that need to be taken into account when making a decision about countermeasures. Each domain is a logical grouping of capability factors which, if all practices are carried out, result in a quality decision-making process for choosing countermeasures. An overview of the model can be seen in Figure 5.2.

For every domain, there is an aim to which it is included in the capability model. Additionally, the capability factors are introduced with an explanation of why these factors are relevant for this domain.

5.1.1 Business

Aim: The necessity for the countermeasure is clear to the organisation. The countermeasure is explainable to ensure the only measures that are needed are taken. The best fit for the organisation is ensured with this.

1. *Choose a countermeasure based on risk.* A risk-based approach provides a firm basis of the relevance of a certain countermeasure.
2. *Comply to laws, regulations and contracts.* Compliance to requirements by laws or other regulations is ensured.
3. *Fit countermeasure in the business.* The countermeasure is fitted within the business processes and integrated in the business to ensure maximum effectiveness.

5.1.2 Bytes

Aim: To make a rational decision about the countermeasures, tools like best-practices and quantifiable measurements are used. These tools in addition to learning from incidents contribute to a rational decision about the countermeasure.

4. *Choose countermeasures that prevent incidents from occurring.* Incidents are prevented and threats are monitored.
5. *Choose countermeasure from best-practices.* In order to choose the most effective and cost-efficient measures, best-practices are used.
6. *Use quantifiable measurements.* Quantified measurements provide rational insights in effective and cost-efficient measures.

5.1.3 Behaviour

Aim: The need for the countermeasure is known throughout the organisation. This ensures that there are no workarounds and that countermeasures are most effective.

7. *Get support for the countermeasure.* Choosing an effective countermeasure needs inclusion of the support in the organisation.
8. *Create awareness about the need for countermeasures.* Awareness about the need for countermeasures ensures the effectiveness of the measure.

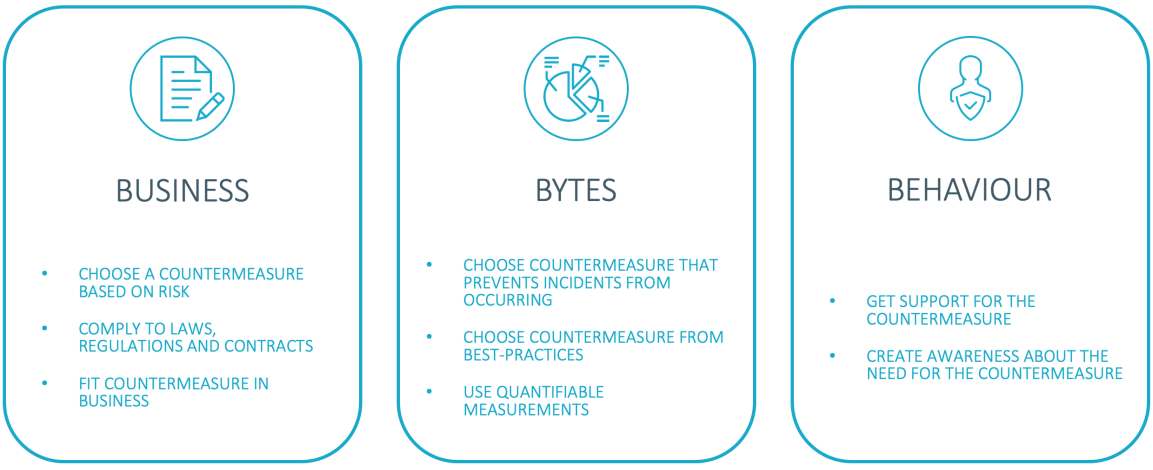


Figure 5.2.: The Decision-Making Capability Model for Countermeasures

5.2 Factor indicator levels

Each capability factor in a domain is measured on their presence by using Factor Indicator Levels (FILs). The FILs in this model are defined by certain practices that are carried out in order to reach the level of existence. These FILs are based on the maturity indicator levels of the C2M2-model by Christopher et al. (2014) and the capability levels of the CMMI-model (CMMI Product Team, 2010).

There are four levels: *incomplete*, *performed*, *managed* and *defined*. Advancing through the levels is straightforward: the organisation needs to show that the practices that are defined in the next level are carried out. The transition from *incomplete* to *performed* is only showing that the capability factor is sometimes taken into account when making a decision. Advancing from *performed* to *managed* is more difficult. Then the maturity factor needs to be taken into consideration always when making a decision and this needs to be shown by documentation and the way of commitment of the organisation to the capability factor. Lastly, progressing from *managed* to *defined* entails even more standardization and monitoring the effectiveness of the decision is taken into account. Furthermore, responsibilities are assigned and resources are allocated to ensure the capability factor to be taken into account when making decisions about countermeasures.

Factor Indicator Level 0 (FIL0) - Incomplete

The model contains no practices for FIL0. At this level the capability factor is entirely not present at decision-making. Therefore, performance at FIL0 means that FIL1 for this capability factor has not been achieved.

Factor Indicator Level 1 (FIL1) - Performed

FIL1 indicates that the factor is thought of sometimes in the decision-making process, which is the only practice of this level. To achieve FIL1 the decision-making process needs to show one or more activities that indicate that the capability factor is taken into account. There is no indication that the activity is institutionalized in the organisation and it is managed. Typically, at FIL1 organisations do not actively repeating the practice.

FIL1 is characterized by a single practice:

1. *The factor is present, but not internalized.* For this level, there are one or more activities that show that the factor is (sometimes) taken into account. To reach FIL1 there is no need for a standardized process in which the factor is present or some way this factor is managed.

Factor Indicator Level 2 (FIL2) - Managed

The next level, FIL2, indicates that the capability factor is initially instituted in the decision-making process. The capability factor is normally taken into consideration when choosing a countermeasure. This is shown by three practices:

1. *The activities are documented.* The activities that are carried out in order to make sure the capability factor is present in the decision-making process are planned and carried out as planned. This is documented to make sure that the activities provide value to the organisation.

2. *Standards have been created to use the factor similarly over time.* In order to be effective in having the capability factor present in the process, it needs to be institutionalized in the process. This is standardized in some way to be able to (re)produce the most effective results.

3. *Resources for having the factor in the decision-making process are available.* Depending on the factor, there is a need for budget and (skilled) people. Resources need to be available when needed to make sure that the capability factor is institutionalized in the decision-making process.

Factor Indicator Level 3 (FIL3) - Defined

At FIL3, the capability factor is deeply rooted in the decision-making process. The organisation is aware that the factor is an important contributor to the process and that it should be instituted in the process. As the organisation knows the importance of the factor, it provides confidence to the decision-making when the factor is taken into account. Practices that support this are:

1. *Measurements are standardised.* The way in which the factor is measured is used in the same way over time. This provides the possibility to learn from every decision in a quantified way.

2. *Appropriate resources are allocated in both amount and skills.* In making a decision the necessary resources are always taken into account and the knowledge needed for implementation and maintaining the countermeasure is reviewed with the available resources in the organisation.

3. *Responsibilities are assigned and defined.* For every measure someone is responsible and what this entails is documented. Taking the responsibility into account, provides an accountability for maintaining and measuring the countermeasure.

4. *Monitoring of the factor is in place to ensure its effectiveness.* The way how the countermeasure is measured is taken into account when making a decision. This ensures that the countermeasure is reviewed on its effectiveness and therefore for its relevance.

5.3 Definition capability model

5.3.1 Business

1. Choose a countermeasure based on risk

Description. A countermeasure is chosen based on a risk. The goal of the countermeasure is to reduce the amount of risk taken by the organisation. The risk-based approach to countermeasures provides effective countermeasures for the organisation.

Table 5.1.: Factor Indicator Levels for risk

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• Countermeasures are taken on an ad-hoc basis • Countermeasures are taken based on a risk
FIL2	• Risks and their importance are identified and documented • Risks are evaluated by chance of occurrence and impact • Relevant stakeholders are contributing to identifying risks • The risk apatite of the organisation is determined
FIL3	• Risks are continuously monitored and adjusted • All risks are quantified with chance of occurrence and impact • Risks are reviewed with the risk apatite in mind • Residual risk is determined after taking a countermeasure • Responsibility for monitoring and evaluating risks is assigned • Stakeholders are continuously involved in evaluating risks

2. Comply to laws, regulations and contracts

Description. The organisation ensures that their countermeasures are on par with laws and other rules and regulations that are relevant to the organisation. Compliance to third-party contracts on security aspects is also taken into account by the organisation.

Table 5.2.: Factor Indicator Levels for compliance

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• Laws, regulations and third-party contracts are checked on security requirements
FIL2	• A registration of relevant laws and regulations is maintained • Third-party contracts are reviewed for security requirements • If needed, ad-hoc measures are taken to achieve compliance
FIL3	• Compliance to laws and third-party contracts is reviewed regularly • Responsibility for compliance is assigned

3. Fit countermeasure in the business

Description. The countermeasure is aligned in the business. It is integrated in the existing business processes of the organisation to match the way-of-working of the organisation.

Table 5.3.: Factor Indicator Levels for business

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• How the countermeasure affects the business process is considered
FIL2	• Countermeasures are integrated in the business process • A budget for recurring security measures is available • Business process owners are also the owner of the countermeasure
FIL3	• How countermeasures contribute to the business objectives is registered • Extra steps/work as result of the countermeasure is minimised

5.3.2 Bytes

4. Choose countermeasure that prevents incidents from occurring

Description. The organisation learns from incidents and takes them into account when choosing countermeasures to prevent the incidents from recurring. Threats are reviewed on their relevance to the organisation in order to prevent them from becoming reality.

Table 5.4.: Factor Indicator Levels for incidents

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• Countermeasures are taken to treat incidents
FIL2	• Incidents are registered • Actions from incidents are registered • Threats to the organisation are identified • Budget for ad-hoc security measures is available
FIL3	• The root cause of incidents is investigated • Known threats are re-evaluated for changes • Incidents in the entire branch are monitored • Countermeasures are reviewed on effectiveness towards the current threats • Threats are shared throughout the organisation • Responsibility for monitoring threats is assigned

5. Choose countermeasure from best-practices

Description. In order to choose a countermeasure best-practices are reviewed for applicability in the organisation. Best-practices can aid in choosing an overall effective and efficient countermeasure for the organisation.

Table 5.5.: Factor Indicator Levels for best-practices

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• A best-practice is considered as source of input for a countermeasure
FIL2	• A best-practice is selected for use that suits the organisation • The best-practice is reviewed with risk assessment in mind
FIL3	• Changes in best-practices are monitored and acted upon • Responsibility about the best-practice is assigned • What is and is not relevant from best-practices is documented

6. Use quantifiable measurements

Description. Countermeasures are measured quantitatively in order to choose the most effective and cost-efficient measure. This quantification provides insights in how effective and cost-efficient the measure is to the organisation in a rational way.

Table 5.6.: Factor Indicator Levels for quantifiable measurements

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• Some quantification is used for selecting countermeasures
FIL2	• Quantified measurements are used for selecting countermeasures • Qualified people produce the quantified measurements • Available data is used as input for the measurements • Quantified effectiveness of current countermeasures are used as input
FIL3	• Standard quantification is repeatedly used for selecting countermeasures • Effectiveness of the countermeasure is periodically reviewed quantitatively • Responsibility for quantification at selecting countermeasures is assigned • Quantified measurements are reviewed on relevance

5.3.3 Behaviour

7. Get support for the countermeasure

Description. To ensure effectiveness of the countermeasure in the organisation, the broad support in the organisation is considered for the countermeasure. Top management needs to support the measure as well as the organisation needs to conform to the countermeasure. This makes the countermeasure more effective in the organisation.

Table 5.7.: Factor Indicator Levels for support

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• A number of people see the need for having the countermeasure in place • Top management is involved in making the decision
FIL2	• Top management supports the chosen countermeasure • Countermeasures are implemented step-by-step to ensure commitment • Time and money for training personnel about the countermeasure is available • Knowledgeable people to implement the countermeasure are identified • The organisation discourages not complying to the countermeasure
FIL3	• The organisation facilitates the way-of-working with the countermeasure • Responsibility is assigned for promoting the countermeasure • Employees are able to explain why the countermeasure is implemented

8. Create awareness about the need for countermeasures

Description. The level of awareness in the organisation affects the countermeasures that can be taken. Therefore, the degree of awareness can limit the decision for a certain countermeasure. In an organisation where the need for a countermeasure is indisputable, different countermeasure can be more effective.

Table 5.8.: Factor Indicator Levels for awareness

Level	Characteristics
FIL0	• Practices are not performed
FIL1	• Security awareness is part of employee training • Ad-hoc awareness sessions are organised
FIL2	• Security behaviour policy is established • Security awareness projects are defined • New countermeasures are explained to the organisation • Resources for improving awareness are available
FIL3	• Responsibility for awareness is assigned • An awareness program has been established • Employees are kept up to date about the relevant countermeasures • Tests on the level of awareness of the organisation are held • Employees are willing to commit to any countermeasure

Part III

Evaluation

6 Validation

> *We all need people who will give us feedback. That's how we improve.*
>
> **— Bill Gates**
> Principal founder of Microsoft

This chapter will validate the Decision-Making Capability Model for Security Countermeasures (DMCMSC) which has been designed and defined in the previous chapters. The goal of validation is to predict how the model will be used and the value it provides in practice (Wieringa, 2014).

The validation is done in two ways: firstly, in section 6.1, follow-up interviews with security consultants are held. The consultants have already seen the entire model as they are part of third round of the Delphi study (see section 4.4). Therefore, in the interviews the main focus is the usability of the model with their clients and the relevance for their clients. Secondly, in section 6.2, two case studies are done in order to validate the DMCMSC with real-world cases. The target of the case studies is to show whether the model provides a good reflection of the real world. This will also show the value of the model to improve the quality of the decision-making.

6.1 Follow-up interviews

The security consultants have been included in the third round of the Delphi study (see section 4.4) and are interviewed to check relevance for their clients. In order to validate the use of the DMCMSC, two of the consultants are interviewed after the Delphi study to gain more in depth information.

6.1.1 Methodology

Similar to the interviews conduced as part of the exploration phase (see section 3.3), the interviews for validation will be conducted using the overview provided by RAND (Harrell and Bradley, 2009). In this case the interviews are used to gain in depth information on how the consultants see the capability model and the usefulness of the model. As different consultants can have different views on this, interviews are chosen as the most effective method.

Table 6.1.: Design of validation interview with security consultants

Phase	Description
Framing the research	
Research question	How can the capability level of the decision-making process about security countermeasures be determined using the created model?
Source	Security Consultants
# respondents	2
Sampling	Convenience sample: *Available consultants are asked.*
Designing questions & probes	
• In what way would you use this model?	
• Could this model help clients improve their decision-making about countermeasures?	
• *In addition:* follow-up questions on the third round of the Delphi study	
Developing the protocol	
Introduction	Security consultants are asked to participate in this research at the office
Ground rules	The interview...
	... will take up 30 minutes.
	... aims to validate the created model.
	... will only be used within the context of the research.
	... is strictly confidential.
	... be recorded in notes.
	... will be reported about in the master thesis, but will be anonymised to safeguard the privacy of the respondent.
Questions & probes	*See questions & probes above*
Closing	No follow-up required
Preparing for the interview	The third round of the Delphi study is filled in
Conducting the interview	The interview guide as described by the protocol will be followed
Capturing the data	Afterwards, the interview will be (partly) transcribed

The main question that is answered in these interviews is: '*How can the capability level of the decision-making process about security countermeasures be determined using the created model?*'. This aim of the interview is broken down into a number of questions in a semi-structured interview. The design of the interview can be found in Table 6.1.

6.1.2 Results

From the interviews it became apparent that the Decision-Making Capability Model for Security Countermeasures is useful, but not to everyone. The model is probably most suitable for bigger projects in order to see how a client operates. One of the respondents noted that the model is more needed for starting consultants as it provides structure to assess the context of the organisation.

The respondents both thought the DMCMSC could be best used by a larger organisation to self-assess their decision-making process. This would help the organisation to improve their decision-making process about countermeasures. A respondent said that the model indicates well what the next steps to improve the decision-making process should be and this would make it easy of organisations to improve.

There was an agreement on whether the model would help clients to improve their decision-making about countermeasures. The respondents thought that this would certainly be the case, mostly because of the awareness-effect the model would have. Client would be more conscious about what they do and do not include in their decision-making process about countermeasures.

6.2 Case studies

In addition to the follow-up interviews with the security consultants, two case studies are performed. Whereas the interviews show how the capability model is of value, the case studies show that the model is valid and that it reflects reality.

6.2.1 Methodology

Two organisations were found willing to participate in a case study. Both case studies followed the same structure in order to be comparable.

1. *Fill out assessment DMCMC.* The CISOs of the organisation are asked to fill out the assessment of the Decision-Making Capability Model for Security Countermeasures (in Microsoft Excel) themselves. This would probably take the CISO about 30 minutes to complete and it may require the CISO to ask around in the organisation.

2. *Discuss the assessment.* The discussion is an unstructured discussion with the CISO to provide room for all sort of feedback on the model. Generally it consist of two parts:

    - *Discuss the use of the model.* The way the model is used is discussed. Aspects like practicality, user friendliness and speed are attended to.

- *Discuss the implications of the outcome.* The DMCMSC provides an overview of the capabilities of the organisation and provides insights in how the organisation could improve. These implications are reviewed on the reflection on the real world. The main issue is to find out whether the DMCMSC reflects reality well and whether the CISO agrees with the outcomes.

6.2.2 Child daycare organisation

Background

The case is a child daycare organisation in The Netherlands. It has more than 200 locations and employs over 2000 people. This organisation is daily affected with protecting the privacy of the children and securing their data. The Security Officer (SO) of the organisation works for three days per week for this organisation and has experience in security for at least three years.

Filling in the assessment took the SO about 15 minutes. He did not need any help or information from other people within his organisation.

Use of the DMCMSC

The SO indicated that he was able to use the DMCMSC quite easily. He thought that he understood well enough what was meant in the model and could answer the questions well. Filling out the assessment was not a problem and he did not need any additional information from the organisations; it could be done by him without problems.

He did mention that in order to be able to fill in the model, the persons doing so should be of a CISO-level or similar. Not all people in the organisation can oversee the entire process of decision-making and therefor are not able to fill in the model. In his opinion this is a requirement for the usefulness of the model.

Upon discussing the details in the model, the SO suggested that some of the practices came somewhat out of the blue. As an example, he stated that the practices in *Risk Management* logically build up, but in *Incidents* some of the practices come out of nowhere. He illustrated this with the practice 'Budget for ad-hoc security measures is available'. In his opinion, it is not logical in the build-up of the levels. However, it is evident to him that this practice is there. Thus, he sees the need for having the practice in place although it does not seem logical.

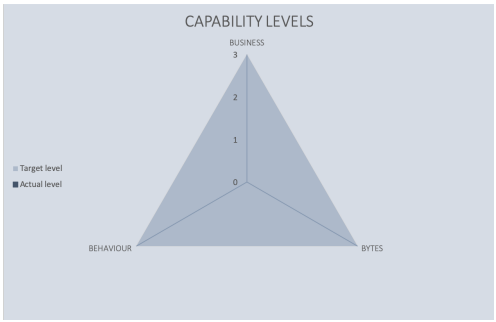
Another aspect is that the answer can only be 'Yes' or 'No'. The SO stated that there always is an area in between. For example, 'Business process owners are also the owner of the countermeasure' is in a number of situations true, but there are situations in which this is not desirable. Some of the countermeasures are top-down and the process owner should simply comply with the countermeasure.

This lead to a discussion about whether the deliberate choice to not do something should be a 'Yes' in the model. On the one hand, this shows that the organisation has thought about the factor of the model and even looked into the practice that should be in place according to the DMCMC. On the other hand, the organisation does not comply with the practice as is presented in the DMCMC, which is approved by a number of experts in practice. The SO stated that when something is deliberately not carried out, this always has a negative effect on the results of the DMCMC which could lead to an unfair view about the organisation.

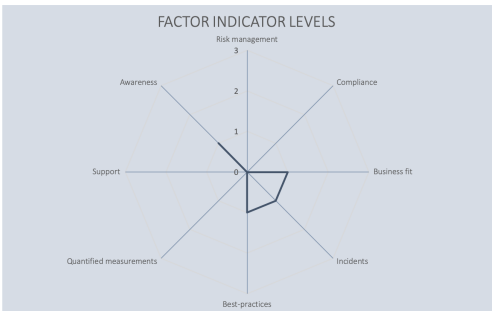
Implication of the outcome

The results-page of the DMCMSC showed that the organisation does not have a high capability level on all aspects, see Figure 6.1. The view this presents is rather negative towards the organisation. The SO, however, firstly stated that this represents the real situation.

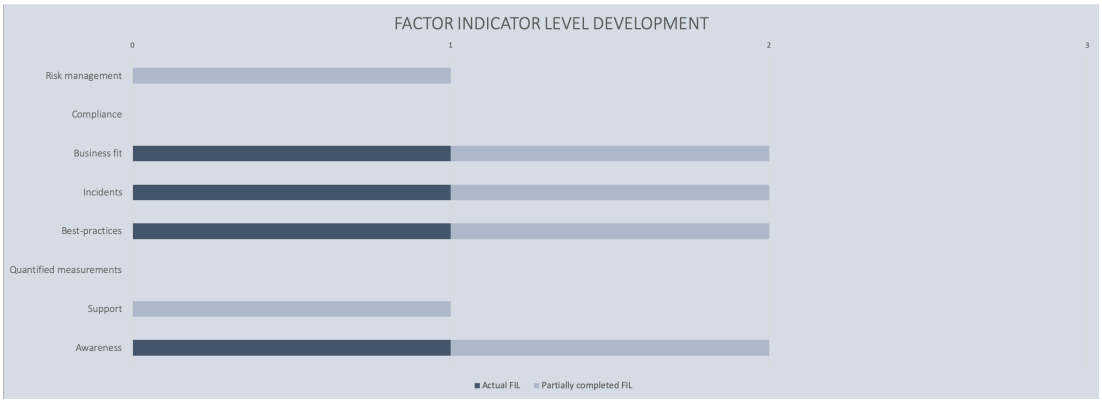
As the SO looked into the results more, he commented that the results do not always resemble the organisation. Some items are more nuanced than simple a harsh score of 0 (or practice is not carried out). The SO wondered how the model calculated the levels in order to better understand why and how a factor could be zero.



(a) Capability levels



(b) Factor Indicator Levels



(c) Factor Indicator Level Development

Figure 6.1.: Results of the first case study

After some explanations on how the model calculates and why the model requires all practices carried out in order to achieve the capability level, the SO stated two things:

- This explanation on how the model works should be included in the tool (Excel-file)
- When one would test it in his organisation, the view the model presents, is probably accurate.

Lastly, the SO indicated that he was most interested in the last graph on the results-page. The 'FIL Development'-graph present what levels are done partly. He therefore knows that in order to become more capable in making decisions about countermeasures, that he can focus on these levels.

6.2.3 Managed security services organisation

Background

The second case study has been done at a managed security services organisation that employs about 100 people. It supplies medium and large clients in the Benelux with services like implementation of ISO27001, security monitoring, penetration tests, incident response. The CISO of this organisation is one of the employees that also provides customers with these services.

The assessment took the CISO about 15 minutes to complete. During the assessment the CISO did not need any additional information from colleagues.

Use of the DMCMSC

During the assessment the CISO had a few questions on how he was supposed fill in the assessment. It was not clear that there should be an answer 'Yes' or 'No', but he did expect an answer of the capability level; 0 to 3. Furthermore, there was no explanation on how the model calculated the score and this should be clearer in the assessment in order to provide value for the CISO. After a small explanation on how the calculation is done and what answers to fill in, the assessment was easily done by the CISO. He did not require any additional information from the organisation or other people in the organisation.

In discussion about the use of the model, the CISO indicated that the assessment is logical. The structure of the different practices was clear and followed each other logically. Sometimes, some practices in FIL2 or FIL3 are done, but not all practices in FIL1 or FIL2 are carried out. This can be the case, but it was no cause for changing the FILs.

One interesting point was the practice "*Countermeasures are taken on an ad-hoc basis*". As the CISO indicated the decision are not done on 'ad-hoc basis', but are made on basis of risk management, the answer to this practice would be 'No'. However, the capabilities of the organisation are much higher than level 0. The description of this practice should probably

be rephrased as "*Countermeasures are structurally taken on ad-hoc basis*" or something similar in order to cope with this.

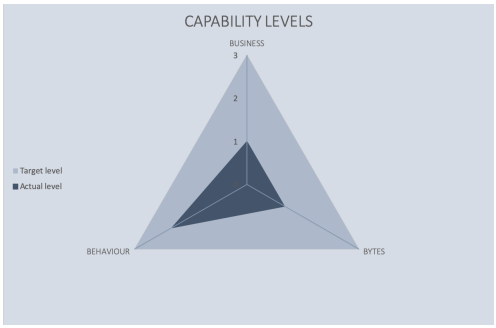
Another point of discussion was the descriptions of *Quantified measurements*. The CISO indicated that he did not understand every practice of this factor fully. He added that this would probably be because his organisation does not use any quantification in choosing the countermeasure.

Lastly, the FIL0 should in the eyes of the CISO not be included in the levels. As there are no practices for this level, he does not need to see it at every factor. The model will automatically assume that the organisation is at FIL0 when every other factor is not carried out.

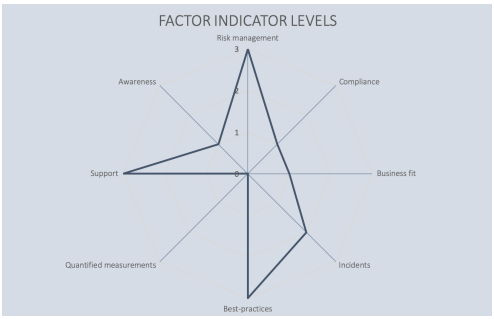
Implications of the outcome

The results of the DMCMC provided that this organisation is generally on FIL1 with a FIL2-level on *Behaviour*, see Figure 6.2.

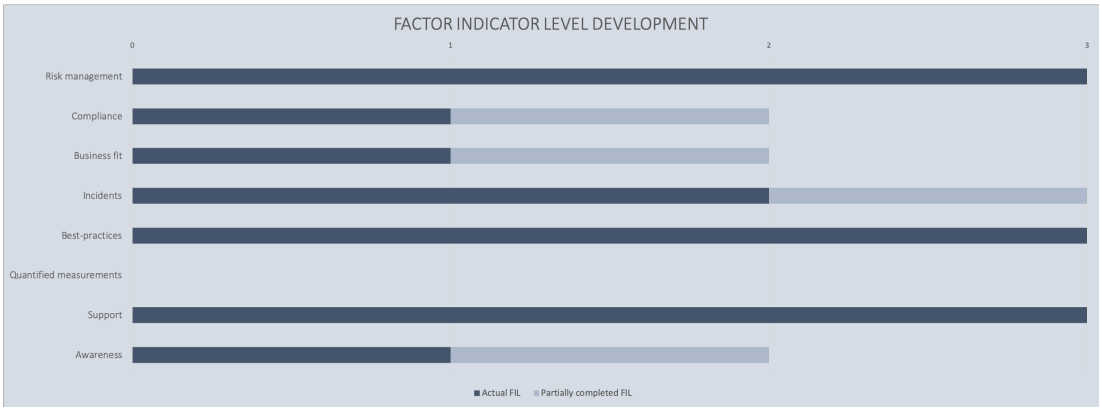
Overall the CISO thought that the results the model presents are grim. Looking at the definitions of the FILs he would expect Business and Bytes to be at FIL2 instead of FIL1. As the model just cuts of any development into level 2 and 3 that is there, the results look very negative. After some discussion on how the model does calculate the level, the CISO could understand the results for the DMCMC.



(a) Capability levels



(b) Factor Indicator Levels



(c) Factor Indicator Level Development

Figure 6.2.: Results of the second case study

The context of the organisation cannot be included in the model currently. The CISO noted that as he works in an organisation that is concentrated primarily on security, he does not need to focus a lot on awareness. The standard level of awareness for people working in security is high on average. A number of practices are therefore not needed in this particular organisation. This again raises the question about the deliberate answer of 'Yes' when it is not done deliberately.

Furthermore, the CISO indicated that after completing the assessment, it was not clear what he should now work on tomorrow in order to improve his capability. There is no important next step. Of course, he could work on adding practices that he now had to answer with 'No', but what should be implemented first?

The graphs presented to the CISO were clear and provided the insights that could be expected. The FIL-development graph was however not obvious on first sight. The CISO asked what the light area meant, but after explaining he noted that this would help him to see the next steps to become more capable in making decisions about countermeasures.

6.3 Implications

This chapter provides a validation of the Decision-Making Capability Model for Security Countermeasures. The question '*How can the capability level of the decision-making process about security countermeasures be determined using the created model?*' is central in this validation. Two methods are used to answer the question: interviews and case studies.

The interviews show that the DMCMSC is a useful tool according to security consultants. It can shed light on the context of the organisation in order to understand the organisation better. Not everyone is suited to use the DMCMSC as one should have the information needed to fill in the assessment. Therefore, security consultants deem it best that responsible persons within an organisation use the DMCMSC. Lastly, the capability model could indeed aid organisations to improve their decision-making about security countermeasures according the security consultants.

Case studies have proven that the DMCMSC does reflect reality. Both of the case studies carried out give a relatively accurate view of the capabilities of the organisation. In both cases the critiques were mostly on the harsh view the model presents. As there is no *grey* area between 'Yes' and 'No', there are still questions on how to score activities that are partly carried out or are deliberately not done. This needs more research and, most importantly, more explanation within the assessment. Furthermore, there are some improvements suggested from the case studies, such as changing the description of a few activities. However, overall the case studies show that the using the DMCMSC is relatively straightforward and that the results are an accurate representation of the capability of the organisation on decision-making about security countermeasures.

The validation shows that the Decision-Making Capability Model for Security Countermeasures is applicable in two kinds of different organisations in the Netherlands. In both cases the assessment is done by a person that can oversee the entire process of information security of the organisation. Seddon and Scheepers (2012) indicates that in similar cases the same results hold, thus can be concluded that within organisations in the Netherlands the DMCMSC does provide accurate and relevant results in order to improve their decision-making about security countermeasures.

7 Discussion

> *Making a wrong decision is understandable. Refusing to search continually for learning is not.*
>
> — **Phil Crosby**
> (Business man)

In the previous chapters of this research the scope of the model is defined, the model is designed and the model is evaluated. This chapter discusses the methods used and investigates in the reliability, validity and limitations of this research. Below, the different phases in this research are discussed, this begins with the exploration phase, followed by the Delphi study and a discussion of the capability model itself. This discussion also includes a reflection on generalisation of this research. Lastly, open questions for future research which arise from this research are discussed.

Throughout this research the methodology by Mettler (2011) has been used. The methodology provided valuable steps in the process of creating a maturity capability model. In the past the methodology of Mettler (2011) has been used by multiple scholars which has proven effectively for designing maturity capability models. Mettler (2011) used three older methods to create an even more effective method to design and create maturity capability models. Although this methodology is useful, it only provided the steps to be taken. The specific steps all used a more detailed methodology in order to be reliable. These steps are elaborated on below.

7.1 Exploration phase

7.1.1 Literature review

The literature review is the first step taken in the design process. A systematic literature review as described by Kitchenham (2004) is carried out. The steps of the methodology of Kitchenham (2004) have been reported explicitly in the thesis. These steps have been proven effective and relevant by a large amount of studies that also used this methodology. As all steps in the SLR are reported on this literature review can be carried out again easily and this would reproduce the same results. The SLR is therefore a very reliable source of information.

There are a few issues on the validity of the SLR, however. The search terms used could have left room for relevant papers that are not included in the SLR now. Although this could be a risk of missing vital information, the search terms are carefully chosen. This was firstly based on the experience of already reading a large number of papers in the subject before conducting the SLR. This provided the insights that several terms have been used for the same concept (e.g. '*cyber security*' and '*cybersecurity*'). Also, some previous work has been used for inspiration of the search terms (e.g. Weishäupl et al., 2015a; Tu and Yuan, 2014). For this reason, the chance of having missed relevant papers is low.

Another point of discussion is the interpretation of the decision-making factors found in literature. All papers found have been read in full and were searched for relevant factors for this research. The exact wording of the factor of the paper has been noted down (and can be found in Appendix B) in order to provide insight in the line of reasoning in this thesis. A number of factors from the papers were changed in order to fit better in the scope of this thesis. Therefore, the meaning of the factor as provided in the papers found could have been changed. This could lead to different interpretation of the factor than originally meant by the author of the paper. The chance that this happened in this thesis is rather high as the SLR was conducted in a limited time. However, this risk reduced by reading the papers multiple times and reporting transparently on the interpretation of the factors.

The main limitation of the SLR was time. The SLR was part of a larger research and it has been conducted in a limited time-frame. Therefore, it can be that some papers have been overlooked or the papers were not thoroughly understood. The limitation of time was the main reason for the exclusion criterion '*Only one of the search terms reflected*'. As a result of this criterion, a number of papers have been excluded from the search. The same result was for the criterion '*Papers that are not in English*'. Because of these criteria, it could be that in a number relevant factors were mentioned that have now been overlooked. The chance of this is low as most factors are mentioned by a number of papers and these have been proven to be the main factors in this area.

7.1.2 Maturity capability models

The second part of the exploration has been reviewing existing maturity capability models. Reproducing this part of the research is less structured as there is no proven methodology to do this (Hillegersberg, 2019). For identifying the different MCMs a number of search terms have been used, but in addition also models were recommended by people from practice and supervisors. This lead to the inclusion criterion '*Widely used in practice*'. Naturally, this criterion will produce different results in a different contexts. Depending on the context different models could have been included in the review.

Reviewing the MCMs was reasonably reliable as the criteria on which the models are reviewed are reported transparently. This method of combining (the same) different criteria was also used in Vermeij (2018) and has proven to be useful in that paper as well as in this research.

The author of this thesis has not used the MCMs in practice and therefore has no experience with using the models. This could lead to a wrong interpretation of the model and therefore the factors derived from the models. As with the SLR, the factors from the MCMs have been reported transparently in order to question the grouping of the decision-making factors about countermeasures. Because of the lack of thorough experience with the models, the chance of wrong interpretation is high. In order to compensate for this, the models were read multiple times and people with (some) experience in (some) of the models have reviewed it.

A major limitation of the research on MCMs is not finding all the relevant models. This limitation is also present because of time constraints in order to produce the entire research. The impact of these discussion points is low as different sources are used to search for relevant factors.

7.1.3 Security consultants

As a third step in identifying factors, security consultants have been interviewed. The interview method was deliberately chosen to provide the most in depth insights. Using the methodology of Harrell and Bradley (2009) provided a structured and proven framework of conducting interviews. All of the steps have been reported in this research. Given the same people and context, the interviews would yield the same results. The interviews have been a reliable source of information in order to identify the relevant decision-making factors.

There are questions on the completeness and validity of the results. Due to the fact that these interviews have been conducted in parallel with the SLR and evaluation of MCMs, not all relevant results have been reached. If the interviews were conducted later in the process, the results of the SLR and the evaluation of MCMs could have been verified in the interviews. Now, the interviews were conducted as an exploration and therefore not resulted in all the relevant factors that were found. On the other hand, if the interviews were used to evaluate the outcomes of the SLR and MCM review, it could have been that a number of factors from practice were missed.

Time has been a limitation for the interviews as well. The consultants are always busy providing services to their clients and therefore did not have a lot of time for an interview. Thus, an interview of a maximum of 30 minutes was conducted instead of going into more detail if there would have been more time. Possibly, this limited the results from the interviews.

Furthermore, the interviews were conducted with security consultants from just one organisation. This definitely resulted in a more one-sided view on making decisions about countermeasures. However, as the interviews were part of the larger exploration, the impact of this has been limited.

7.2 Delphi study

The decision-making factors about countermeasures found are tested in practice with a Delphi study. This has resulted in a three-round Delphi study with 12 initial panellists who have helped shape the Decision-Making Capability Model for Security Countermeasures. The method of a Delphi study was selected in order to be able to quickly improve the model by participants in multiple companies and different locations. According to Okoli and Pawlowski (2004), the Delphi sturdy is a good tool for development of an artefact.

However, literature also shows that Delphi studies have known issues. Linstone and Turoff (1975) describe a number of failures that are common for Delphi studies. One of most problematic issues is imposing the monitor's view and perceptions on the respondents. In this research, that issue has been recognised and the surveys have been reviewed on this aspects specifically at least once during the composition of the survey. Other mentioned issues by Linstone and Turoff (1975) are using poor techniques of summarising and not exploring disagreements enough. In order to cope with this a tool, Spilter, has been used. Spilter has been used to conduct Delphi studies in the past and has been proven useful. The techniques of summarising are as they are presented in Spilter and are therefore tested. Disagreements are always elaborated on by the panellists and this made it possible to gain in depth insights.

Although Spilter has been used multiple times for Delphi studies before, it has not proven to be perfect. For example, there were only a few different kind of questions that were allowed to be viewed by all the panellists during the Delphi round. Whereas the Delphi study aims to reach consensus by openly discussing the answers, this was not always possible within Spilter. Furthermore, because of the anonymity functionality of Spilter, it was not possible to gain information by looking at the answers of a single panellist. This blocked insights in whether people in a large organisation have different views on the topic than in small companies, or that a certain industry has a particular view.

The sample of participants to the Delphi study was mostly based on people who were willing to participate within the network of the researcher and the company the research was conducted at. This provided a sample with panellists only based in The Netherlands and (almost) all were clients of the company. This could have provided a one-sided view on the subject. By having a few panellists that came from a different background, this effect has been minimised. There is no indication that the sample limited the discussion.

The surveys have only been tested on usage and clearness, not on validity. This has resulted in a few issues. In the first round, the definitions of the decision-making factors were not clear and therefore a number of different perspectives have been used by the panellists. When the definitions had been tested and improved beforehand, the results of the first survey would have been even more useful and valid. The second survey was not entirely complete, as one of the factors was missing from two of the questions. This mistake has been fixed after the

first four panellists had answered the questions. By testing the survey more, this mistake could have been prevented. The third and final survey did not reveal any of these issues.

7.3 The capability model

In composing the capability model, reliable methods have been used. The main approach has been as Mettler (2011) described and his research is based on a number of other methodologies to create maturity capability models. In addition the use of a Delphi study to create a model has been proven successful in the past (e.g. Van Dijk, 2017; Vermeij, 2018). In this research all choices are elaborated on transparently and can be reconstructed with the information in this research and the appendices.

There are a number of open questions on the validity of the capability model as it is now. In this research it has been out of scope to confirm whether the model really tests what it is supposed to measure. Although, a lot of effort has been made to ask people from practice what the model should look like and what it should ask and therefore this point is somewhat managed. Furthermore, the factors present in the model are derived from a number of sources. It cannot, however, be made certain that all of these factors improve the quality of the decision-making. This is only not measured within the scope of this research. The factors probably are somewhat intertwined, however it is not known how and how much.

Two of the factors need more discussion. Firstly, risk management is included in the model as one of the decision-making factors about countermeasures, however one could argue that without risk management the entire model would not exist. To almost everyone risk management is the basis on which the decision can be build and without it, there is probably not a question of what countermeasure to implement. Secondly, awareness is always an interesting factor. Without any awareness there is definitely no question on countermeasures, because then countermeasures are not even needed. For this reason it was first excluded from the model in the exploration phase. However, in the Delphi study it was included again due to questions of the panellists. They did see awareness as an important factor in order to be able to implement countermeasures.

Another element that needs discussion, is the way in which answers can be given in the model. Currently a practice can be carried out or simply not carried out; the answer is 'Yes' or 'No' and no grey area in between. The question, however, remains: '*Can every practice be answered by Yes or No?*'. Some people might answer a 'Yes' quickly, even when the practice is not done in full, which provides a rather positive view as a result or completely the opposite. It can also be that some practice is deliberately *not* done by the organisation for some reason. One could argue then that the practice is carried out (because we know why it is not) and it therefore opens up the possibility to have a much higher capability score in the model. However, one could also argue contrary, because without the practice the quality of decision-making is not improved. This issue needs more research and it could be that the model can be much improved by adding a answer level between 'Yes' and 'No'.

7.4 Future research

In order to become more secure in the digital world, this research provides a next step to improve the quality of the decision-making process. There are still plenty of questions that still need answers.

Firstly, for the Decision-Making Capability Model for Security Countermeasures to be most effective, the use needs to be proven. Next steps in this are researching the influence the decision-making factors have on each-other and on the resulting decision. Does every factor contribute to a better decision? Is every factor a necessity in this model? Afterwards, it should be measured that the model indeed helps making more decisions that are more effective and more cost-efficient. Researching this will take time, as the implementation of countermeasures and then evaluating their effectiveness will probably take close to three years.

Another aspect that can be looked into further, is the usage of the model. Can the model help decision-makers to base their case stronger and therefore make better decisions? To what extend does this capability model help the decision-maker or is the gut feeling of the decision-maker as good as the model or maybe even better? That research will provide answers on which the model could improve or be more firmly based as a model that helps making quality decisions.

A bit more out of the scope of this research, there is still a question of how the process of selecting a countermeasure look like (also stated by Weishäupl et al., 2018). It would be very interesting to look at multiple organisations and sketch their processes in order to be able to compare those. This could lead to process-steps that are relevant to make good decisions. Furthermore, this could prove that some processes (or steps) are vital in selecting the best countermeasures for the organisation.

Conclusion

8

> *In any moment of decision, the best thing you can do is the right thing. The worst thing you can do is nothing.*
>
> **— Theodore Roosevelt**
> 26^{th} President of the United States

This research has presented a multi-method approach to develop a capability model for the decision-making process of countermeasures in information security. Through multiple methods, combining literature and practice, eight factors have been identified that are of vital importance to the decision-making process. These decision-making factors are tested in the capability model on their presence in the decision-making process of the organisation.

The goal of this research was to '*Improve security risk management by designing a capability model that gives a performance indicator of decision-making in order to rationally reduce risks to an acceptable level*'. To achieve this goal four sub-questions are answered in this research.

> **SQ1.** What does the overall process of risk management look like and where does the process of deciding about security countermeasures fit in?

Chapter 2 describes the context of information security. Organisations nowadays are faced with threats to their assets. In order to remain in business, organisations need to take countermeasures or controls to stay secure. Staying secure in the changing environment is not easy, thus organisations need to manage it constantly.

Effective information security is different to every organisation. It is critical that organisations have a good IS policy, commitment of resources and a strong security culture to be effective. There are tools available that help organisations to achieve this in their information security management, like standards such as ISO/IEC27000-series and quantified measurements such as Return on Security Investment, Return on Attack and defence trees.

Most importantly, to manage information security well, organisations need to use risk management. Managing the risks to the organisation provides insight in what the organisation should protect. This is done by repeating a Plan, Do, Check, Act-cycle every year. Part of this is doing risks assessments and treating the risks that are above the risk appetite of the organisation in order to lower the risks. At that moment, certain countermeasures need to be chosen in order to treat the risk to an acceptable level. Currently, there is no standard process for organisations to do so and it is not known what is important to take into account when making this decision.

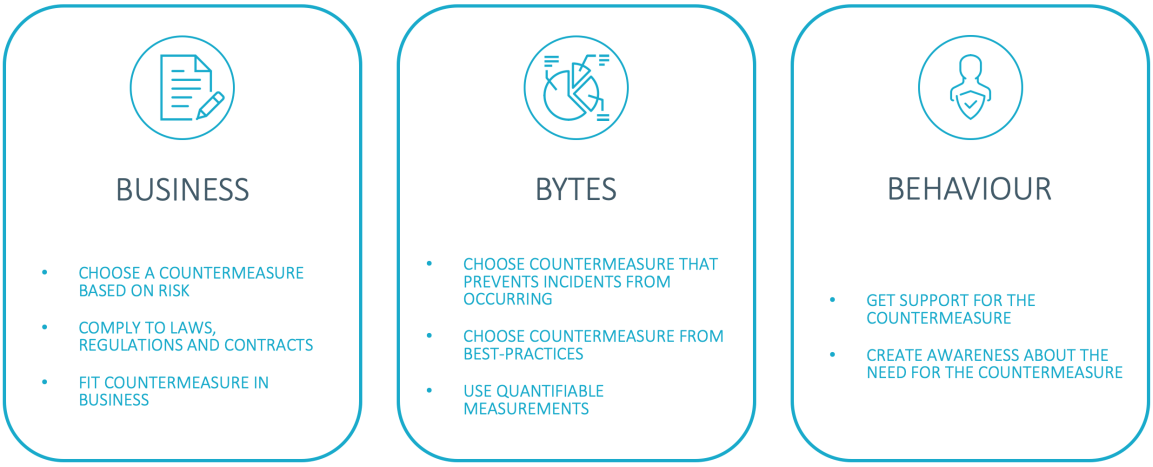


Figure 8.1.: Final factors in the Decision-Making Capability Model for Security Countermeasures

> **SQ2.** What factors should be taken into account for the decision-making process about security countermeasures?

In order to answer this second question, in Chapter 3 three different sources are reviewed as a first step. This chapter described a systematic literature review which included 500 papers, a review of 6 maturity models and interviews with 5 security consultants. In using these sources an initial list of eight important decision-making factors to the selection of countermeasures is identified.

Afterwards, a Delphi study with 12 initial panellists from practice is carried out in Chapter 4. The first survey was completely on testing the factors found in practice and changing the factors to reflect the important points from practice. This has resulted in the integration of two decision-making factors into the other factors and the addition of two factors that were not included before. The final list of decision-making factors about countermeasures can be seen in Figure 8.1.

The last survey revealed that the factors '*Choose a countermeasure based on risk*' and '*Comply to laws, regulations and contracts* are most important to the panellists. These factors show the reason for implementing a countermeasure in the organisation. It can be concluded that making a well-based decision is important to the panellists. On the other hand, quantified measurements are chosen by none of the panellists as one of the top three most important decision-making factors. This is remarkable as using quantified measurements in the decision-making process about countermeasures is the most important factor from literature. This shows the gap there still is between science and practice clearly.

SQ3. How can be determined to what extent a factor, found in SQ2, is present in the decision-making process?

In the second and third round of the Delphi study, also reported in Chapter 4, it is discussed how the decision-making factors can be measured. The panellists provided all kinds of indicators for the factors which are included in the different Factor Indicator Levels of the capability model. Each of the factors are described by a number of activities that can be carried out in an organisation which show that the factor is considered in the decision-making process.

The Decision-Making Capability Model for Security Countermeasures uses four Factor Indicator Levels (FILs), which are based on the CMMI-model (CMMI Product Team, 2010) and the C2M2-model (Christopher et al., 2014). The lowest FIL entails no practices and the highest FIL describes practices that cumulative with the levels below indicate a high capability of including the factor in the decision-making process.

Most of the FILs are agreed upon by the panellists in the Delphi study. There are still a few improvements that can be made in order to be even more concrete. These improvements are mostly textual, but there are some that need more work. Specifically, the factor '*Choose countermeasures that prevents incidents from occurring*' is now more about managing incidents than about preventing incidents according the panellists.

SQ4. How can the capability level of the decision-making process about security countermeasures be determined using the created model?

The Decision-Making Capability Model for Security Countermeasures (DMCMSC) is described in Chapter 5. The model consists of three domains and eight decision-making factors, see Figure 8.1. Each factor is defined by four Factor Indicator Levels in which one or more practices have to be shown in order to achieve that capability level.

The DMCMSC is created in Microsoft Excel in order to make assessments of organisations possible. Case studies have shown that the model is easy to use and instinctive. The model is most relevant to self-assess the capability of the decision-making process of countermeasures in larger organisations. The model can help to identify gaps in the process and improve the process by implementing practices that currently are not carried out in the organisation.

From the interviews and case studies to validate the model, in Chapter 6, became clear that there is still room for improvement. The model gives a harsh, however fair, view of the capability of the organisation. One of the reasons for this is that the model only allows 'Yes' or 'No' as answers. An area between this could improve the applicability of the model.

Main research question: What factors should a capability model include that assesses the decision-making process about security countermeasures?

In this research, the Decision-Making Capability Model for Security Countermeasures has been created. Decision-makers indicate that the model is useful and relevant for organisations to self-assess their decision-making process of countermeasures. The decision-making factors have been found in multiple sources that all discuss their importance towards improved information security. Thus can be concluded that the factors included in the DMCMSC are relevant for decision-making in information security.

Furthermore, the model has been tested in two completely different organisations in the Netherlands. Both cases present accurate information on the decision-making process about security countermeasures. It can be concluded that in similar contexts the DMCMSC delivers the same accurate and relevant results for organisations.

The Decision-Making Capability Model for Security Countermeasures presents accurate insights about the decision-making process of the organisation. This provides organisations with them means to improve their process further and being more capable of selecting the appropriate set of security countermeasures. In term, the countermeasures secure the organisation to let their business thrive with low risk of being put out of business.

Bibliography

Al Awawdeh, Shadi and Abdallah Tubaishat (2014). „An information security awareness program to address common security concerns in IT unit“. In: *ITNG 2014 - Proceedings of the 11th International Conference on Information Technology: New Generations*. IEEE, pp. 273–278 (cit. on p. 107).

Alreemy, Zyad, Victor Chang, Robert Walters, and Gary Wills (2016). „Critical success factors (CSFs) for information technology governance (ITG)“. In: *International Journal of Information Management* 36.6, pp. 907–916 (cit. on pp. 15, 17, 107).

Bernik, Igor and Kaja Prislan (2016). „Measuring information security performance with 10 by 10 model for holistic state evaluation“. In: *PLoS ONE* 11.9, pp. 1–33 (cit. on p. 107).

Bistarelli, Stefano, Fabio Fioravanti, and Pamela Peretti (2006). „Defense trees for economic evaluation of security investments“. In: *Proceedings - First International Conference on Availability, Reliability and Security, ARES 2006*. Vol. May 2016, pp. 416–423 (cit. on pp. 16, 17).

Bistarelli, Stefano, Marco Dall'Aglio, and Pamela Peretti (2007). „Strategic Games on Defense Trees“. In: *Formal Aspects in Security and Trust*, pp. 1–15 (cit. on p. 17).

Bobbert, Yuri and Hans Mulder (2015). „Governance Practices and Critical Success Factors Suitable for Business Information Security“. In: *2015 International Conference on Computational Intelligence and Communication Networks, CICN 2015*, pp. 1097–1104 (cit. on p. 106).

Bojanc, Rok, Borka Jerman-Blažič, and Metka Tekavčič (2012). „Managing the investment in information security technology by use of a quantitative modeling“. In: *Information Processing and Management* 48.6, pp. 1031–1052 (cit. on pp. 14, 15, 20–22).

Caralli, Richard A., Julia H. Allen, James F. Stevens, Bradford J. Willke, and William R. Wilson (2004). *Managing for Enterprice Security*. Tech. rep. Carnegie Mellon Software Engineering Institute, pp. 1–55 (cit. on p. 106).

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan (2004). „A model for evaluating IT security investments“. In: *Communications of the ACM* 47.7, pp. 87–92 (cit. on pp. 15, 16).

Cavusoglu, Huseyin, Srinivasan Raghunathan, and Wei T. Yue (2008). „Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment“. In: *Journal of Management Information Systems* 25.2, pp. 281–304 (cit. on p. 5).

Chehrehpak, M., S.P. Afsharian, and J. Roshandel (2014). „Effects of implementing information security management systems on the performance of marketing and sales departments“. In: *International Journal of Business Information Systems* 15.3, pp. 291–306 (cit. on p. 4).

Christopher, Jason D., Dale Gonzalez, David W. White, et al. (2014). „Cybersecurity Capability Maturity Model (C2M2)“. In: *Department of Homeland Security* February, pp. 1–76 (cit. on pp. 32, 35, 44, 63, 66, 93, 111).

CMMI Product Team (2010). „CMMI for Development, Version 1.3: Improving Processed for Better Products and Services“. In: *Carnegie Mellon University, Software Engineering Institute* November (cit. on pp. 5, 32–34, 44, 63, 66, 93, 111).

Cremonini, Marco and Patrizia Martini (2005). „Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)“. In: *4th Workshop on the Economics of Information Security*, p. 4 (cit. on p. 16).

Dalkey, Norman C. and Olaf Helmer (1963). „An experimental application of the Delphi method to the use of experts“. In: *Management Science* 9.3, pp. 458–467 (cit. on p. 46).

Daneva, Maya (2006). *Applying Real Options Thinking to Information Security in Networked Organizations*. Tech. rep. Enschede: Centre for Telematics and Information Technology, University of Twente (cit. on p. 16).

De Bruin, Tonia and Michael Rosemann (2005). „Towards a Business Process Management Maturity Model“. In: *ECIS 2005 Proceedings of the Thirteenth European Conference on Information Systems*. 26-28 May, pp. 1–12 (cit. on pp. 7, 46).

Department for Digital, Culture, Media and Sport (2018). *Cyber Security Breaches Survey 2018*. London (cit. on p. 3).

Dor, Daniel and Yuval Elovici (2016). „A model of the information security investment decision-making process“. In: *Computers and Security* 63, pp. 1–13 (cit. on pp. 4, 15, 22).

Ekelhart, Andreas, Stefan Fenz, and Thomas Neubauer (2009). „Ontology-based decision support for information security risk management“. In: *Proceedings of the 4th International Conference on Systems, ICONS 2009*, pp. 80–85 (cit. on pp. 4, 22).

Fenz, Stefan, Andreas Ekelhart, and Thomas Neubauer (2011). „Information Security Risk Management : In Which Security Solutions Is It Worth Investing?“ In: *Communications of the Association for Information System* 28.May, pp. 329–356 (cit. on pp. 4, 22).

Gartner, Inc. (2018). *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*. `https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019`. [Online; accessed November 28, 2018] (cit. on p. 3).

Gashgari, Ghada, Robert Walters, and Gary Wills (2017). „A Proposed Best-practice Framework for Information Security Governance“. In: *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pp. 295–301 (cit. on p. 107).

Gordon, Lawrence A. and Martin P. Loeb (2002). „The economics of information security investment“. In: *ACM Transactions on Information and System Security* 5.4, pp. 438–457 (cit. on pp. 5, 15).

Gordon, Lawrence A., Martin P. Loeb, and William Lucyshyn (2003). „Information Security Expenditures and Real Options: A Wait-and-See Approach“. In: *Computer Security Journal* XIX.No. 2, Spring (cit. on p. 16).

Harrell, Margaret C. and Melissa A. Bradley (2009). *Data Collection Methods: Semi-Structured Interviews and Focus Groups*. Santa Monica, CA.: RAND National Defense Research Instution, p. 148. arXiv: `0706.1401` (cit. on pp. 39, 75, 87).

Hillegersberg, Jos van (2019). „The Need for a Maturity Model for Maturity Modeling“. In: *The Art of Structuring*, pp. 145–151 (cit. on pp. 33, 86).

ISACA (2012). *COBIT 5*. `www.isaca.org` (cit. on pp. 13–15, 19, 32, 34, 35, 111).

ISO/IEC (2013a). *ISO/IEC 27001:2013(en)*. Switserland (cit. on pp. 15–23).

– (2013b). *ISO/IEC 27002:2013(en)*. Switserland (cit. on pp. 18, 21, 23).

– (2015). *The Process Approach in ISO 9001:2015*. www.iso.org/tc176/sc02/public. Switserland (cit. on p. 18).

– (2018a). *ISO 31000:2018(en) - Preview*. https://www.iso.org/obp/ui/{#}iso:std:iso:31000:ed-2:v1:en. [Online; accessed January 18, 2019] (cit. on pp. 17, 18).

– (2018b). *ISO/IEC 27000:2018(en)*. https://standards.iso.org/ittf/PubliclyAvailableStandards/. Switserland (cit. on pp. 3, 13, 14, 18).

Kajava, Jorma and Reijo Savola (2005). „Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes". In: *Proceedings of the European University Information Systems (EUNIS)* (cit. on p. 16).

Kitchenham, Barbara (2004). *Kitchenham_Procedures for Performing Systematic Reviews*. Tech. rep. Keele: Keele University, pp. 1–28. arXiv: 339:b2535 (cit. on pp. 27, 28, 85).

Kong, Hee Kyung, Tae Sung Kim, and Jungduk Kim (2012). „An analysis on effects of information security investments: A BSC perspective". In: *Journal of Intelligent Manufacturing* 23.4, pp. 941–953 (cit. on pp. 15, 17, 107).

Linstone, Harold A. and Murray Turoff (1975). *The Delphi Method: Technology and Applications*, p. 616. arXiv: 0-201-04294-0 (cit. on pp. 45, 46, 88).

Mayer, Janice and Leonardo Lemes Fagundes (2009). „A model to assess the maturity level of the risk management process in information security". In: *2009 IFIP/IEEE International Symposium on Integrated Network Management-Workshops, IM 2009* 5, pp. 61–70 (cit. on pp. 32, 36, 111).

McAfee (2018). *Economic Impact of Cybercrime – No Slowing Down* (cit. on p. 3).

Mettler, Tobias (2011). „Maturity assessment models: a design science research approach". In: *International Journal of Society Systems Science* 3.1/2, p. 81 (cit. on pp. 6–8, 33, 46, 85, 89, 103).

NCTV (2019). *Cybersecuritybeeld Nederland 2018*. Tech. rep., pp. 1–88 (cit. on p. 3).

Nicho, Mathew (2012). „An Optimized Dynamic Process Model of IS Security Governance Implementation". In: *CONF-IRM 2012 Proceedings*, p. 20 (cit. on p. 106).

– (2018). „A process model for implementing information systems security governance". In: *Information and Computer Security* 26.1, pp. 10–38 (cit. on p. 106).

NOS (2018). *Zware DDoS-aanvallen: wie, wat, waar en waarom?* https://nos.nl/artikel/2214400-zware-ddos-aanvallen-wie-wat-waar-en-waarom.html. [Online; accessed November 28, 2018] (cit. on p. 3).

Okoli, Chitu and Suzanne D. Pawlowski (2004). „The Delphi Method as a Research Tool: An Example, Design Considerations and Applications". In: *Information & Management* 42.1, pp. 15–29. arXiv: 0-201-04294-0 (cit. on pp. 47, 48, 88).

Panaousis, Emmanouil, Andrew Fielder, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi (2014). „Cybersecurity Games and Investments: A Decision Support Approach". In: *International Conference on Decision and Game Theory for Security*. Springer, Cham., pp. 266–286 (cit. on pp. 4, 16).

Papelard, Talitha and Yuri Bobbert (2018). *Critical Success Factors for Effective Business Information Security*. Dialoog Publishing, pp. 1–359 (cit. on pp. 15, 17, 107).

Partida, Alberto and Jean-Noel Ezingeard (2007). „Critical Success Factors and Requirements for Achieving Business Benefits from Information Security“. In: *Proceedings of European and Mediteranian Conference on Information Systems 2007 (EMCIS2007)* (cit. on p. 107).

Paulk, Mark C., Bill Curtis, and Mary Beth Chrissis (1993). „Capability Maturity Model , Version 1.1“. In: *IEEE Software* 10.4, pp. 18–27 (cit. on pp. 32, 33).

Pöppelbuß, Jens and Maximilian Röglinger (2011). „What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management“. In: *European Conference on Information Systems 2011 Proceedings. 28* (cit. on p. 33).

Rabionet, Silvia E (2011). „How I Learned to Design and Conduct Semi-structured Interviews: An Ongoing and Continuous Journey“. In: *Qualitative Report* 16.2, pp. 563–566 (cit. on p. 39).

Rjaibi, Neila, Latifa Ben Arfa Rabai, Anis Ben Aissa, and Ali Mili (2013). „Mean Failure Cost as a Measurable Value and Evidence of Cybersecurity“. In: *International Journal of Secure Software Engineering* 4.3, pp. 64–81 (cit. on p. 16).

Rowe, Gene and George Wright (1999). „The Delphi technique as a forecasting tool: Issues and analysis“. In: *International Journal of Forecasting* 15.4, pp. 353–375 (cit. on p. 46).

Saleh, Malik F. (2011). „Information Security Maturity Model“. In: *International Journal of Computer Science and Secuirty (IJCSS)* 5.3, pp. 316–337 (cit. on pp. 32, 35, 36, 111).

Sana, Nick (2019). *How CISOs Can Demonstrate Business Value*. `https://www.securityweek.com/how-cisos-can-demonstrate-business-value`. [Online; accessed January 31, 2019] (cit. on p. 4).

Seddon, Peter B. and Rens Scheepers (2012). „Towards the improved treatment of generalization of knowledge claims in IS research: Drawing general conclusions from samples“. In: *European Journal of Information Systems* 21.1, pp. 6–21 (cit. on pp. 44, 83).

Skulmoski, Gergory J., Francis T. Hartman, and Jennifer Krahn (2007). „The Delphi Method for Graduate Research“. In: *Journal of Information Technology Education* 6, pp. 1–21. arXiv: `0-201-04294-0` (cit. on pp. 46, 47).

Smits, Daniel and Jos Van Hillegersberg (2015). „IT governance maturity: Developing a maturity model using the delphi method“. In: *Proceedings of the Annual Hawaii International Conference on System Sciences* 2015-March, pp. 4534–4543 (cit. on p. 46).

Sonnenreich, W, J Albanese, and B Stout (2006). „Return on security investment (rosi)-a practical quantitative model“. In: *Journal of Research and Practice in Information Technology* 38.1, pp. 45–56 (cit. on p. 16).

Stikvoort, Don (2010). „SIM3 : Security Incident Management Maturity Model“. In: 2015.September, pp. 1–11 (cit. on pp. 32, 38, 111).

Stoneburner, Gary, Alice Goguen, and Alexis Feringa (2002). *Risk Managagement Guide for Information Technology Systems*. Tech. rep. National Insitute of Standards and Technology (NIST) (cit. on pp. 15, 17, 35).

The Guardian (2018). *Facebook says 14m accounts had personal data stolen in recent breach*. `https://www.theguardian.com/technology/2018/oct/12/facebook-data-breach-personal-information-hackers`. [Online; accessed November 28, 2018] (cit. on p. 3).

Torres, Jose M, Jose M Sarriegi, Javier Santos, and Nicolás Serrano (2006). „Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness“. In: *International Conference on Information Security*. Berlin: Springer, pp. 530–545 (cit. on pp. 13, 14).

Tu, Zhiling and Yufei Yuan (2014). „Critical Success Factors Analysis on Effective Information Security Management : A Literature Review“. In: *Twentieth Americas Conference on Information Systems (Amcis)*. Savannah, pp. 1–13 (cit. on pp. 86, 106).

Van Dijk, Friso Willem (2017). „Adopting the Cloud: A multi-method approach towards developing a cloud maturity model“. Master Thesis. University of Twente (cit. on pp. 46, 89).

Van Os, Rob (2016). „SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers“. In: p. 74 (cit. on p. 51).

Vermeij, Jaap (2018). „Creating an IT risk maturity model for distributed ledger applications“. Master Thesis. University of Twente (cit. on pp. 46, 86, 89).

Vodafone (2017). *Strong Cyber Security drives growth & innovation*. Tech. rep. Vodafone (cit. on p. 4).

Von Solms, Basie and Rossouw Von Solms (2004). „The 10 deadly sins of information security management“. In: *Computers and Security* 23.5, pp. 371–376. arXiv: `arXiv:1011.1669v3` (cit. on pp. 15, 17, 107).

Weishäupl, Eva, Emrah Yasasin, and Guido Schryen (2015a). „A multi-Theoretical literature review on information security investments using the resource-based view and the organizational learning theory“. In: *International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015*, pp. 1–22 (cit. on p. 86).

– (2015b). „It Security Investments Through the Lens of the Resource-Based View : a New theoretical model and literature review“. In: *Ecis* 2014, pp. 1–19 (cit. on p. 4).

– (2018). „Information security investments: An exploratory multiple case study on decision-making, evaluation and learning“. In: *Computers and Security* (cit. on pp. 4, 5, 90).

Wieringa, Roel (2014). *Design science methodology: for Information Systems and Software Engineering*. Enschede: Springer, p. 332 (cit. on pp. 5, 6, 75).

Yu Wu (2007). „Effects of IT Governance on Information Security“. Doctoral thesis. University of Central Florida, pp. 1–148 (cit. on p. 106).

Zafar, Humayun, Jan G. Clark, Myung Ko, and Yoris A. Au (2011). „Critical Success Factors for an Effective Security Risk Management Program: An Exploratory Case Study at a Fortune 500 Firm“. In: *AMCIS Proceedings*, pp. 1–11 (cit. on p. 106).

Zhiling, Tu (2015). „Effective Information Security Management: A Critical Success Factors Analysis“. Doctoral thesis. McMaster University, pp. 1–181 (cit. on p. 106).