ZERO TRUST MATURITY MATTERS

MODELING CYBER SECURITY FOCUS AREAS AND MATURITY LEVELS IN THE ZERO TRUST PRINCIPLE

MASTER'S THESIS

VERSION 1.0

FEBRUARY 2018

Modderkolk, Michel, Department of Information and Computer Science, Utrecht University
Princetonplein 5, Buys Ballot Gebouw, 3584 CC Utrecht, Netherlands,
m.g.modderkolk@students.uu.nl, *m.modderkolk@outlook.com*, *michel@legalit.me*

Universiteit Utrecht

LegalIT

1st Supervisor
Prof. Dr. Sjaak Brinkkemper
s.brinkkemper@uu.nl
Utrecht University

2nd Supervisor
Dr. Marco Spruit
m.r.spruit@uu.nl
Utrecht University

ABSTRACT

Society is getting more dependent from information technologies - which means that the Confidentiality, Integrity and Availability (CIA) must be guaranteed -, thus the cybersecurity of information systems needs to be improved. At the current date, the complexity of networks has increased exponentially. On top of that, networks will keep extending well outside the controllable borders of enterprises. To solve this problem, enterprises must start letting go of Trust but Verify and start embracing the Zero Trust principle. This research created a Zero Trust Maturity Model (ZeTuMM) that enterprises should use to start with the Zero Trust principles implementations, as well as grow in their Zero Trust maturity. After testing this model at various companies, this research serves as a road sign to continue the work on Zero Trust cybersecurity.

Keywords: Zero Trust, Maturity Model, Cybersecurity, Cyber Security, Information Security, Focus Areas

ACKNOWLEDGEMENTS

The last five years of my life were moving and informative. Never in my life I have experienced and learned so much. Certain aspects of my life went good and other were messed up good. The road to completion of my thesis was not always that easy and during my project there were certain setbacks. Sometimes it was hard to find the motivation to finish my thesis – but in the end – I did finish it and I am proud of doing so. I can only hope that you – the reader – will enjoy this with pleasure, as it was years of hard work, dedication and perseverance.

Firstly, I want to thank all the professors at the University Utrecht who guided me. Especially, I want to thank them for keeping believing in me. They let me make my mistakes and become the person I am today. Especially I want to thank Prof. Dr. Sjaak Brinkkemper, Dr. Marco Spruit, Dr. Slinger Janssen and Dr. Fabiano Dalpiaz.

Furthermore, I want to thank two companies that were case study participants. It's amazing what I have learned and seen at those companies. I feel honored that you gave me the opportunity to validate my master's thesis research.

Finally, I want to thank my family and friends for believing in me and helping me stay motivated to finish my master. Notably my reviewer and friend Nicky van Tongeren.

TABLE OF CONTENTS

List of Figures

List of Tables

1 INTRODUCTION

Civilians, governments and enterprises are getting more and more dependent from IT to complete an increasing amount of basic functions. Since the world started changing to the digital information era information and IT became valuable and needed to be protected. These days not-functioning of IT and compromised information can have serious impact on the operation of enterprises and society as a whole (NCSC, 2014). Most enterprises are not aware of such threats and do not have measures against them, as can be seen in larger enterprises where even (the board of) directors of larger enterprises do not participate in information security activities, even though cyberrisks are a severe present danger (PWC, 2014). This especially applies for SMEs, since they do not have policies in place to apply information security (Syntens, 2006).

> *Information security: to protect the confidentiality, integrity and availability of Information assets, whether in storage, processing or transmission (M. Whitman & Mattord, 2011)*

The goal of information security is to ensure that all information stored in information systems are and will remain Confidential, Integer and Available (CIA) (J. M. Anderson, 2003). It should be achieved with the use of policy application, education, awareness via training, and technology. Not only is there the threat that has to do with information security. Since the rise of the internet there are new threats, so called cybercrimes. Most enterprises do not recognize these threads at hand (Brummelkamp, 2009). Even though almost all enterprises own valuable digital assets (NCSC, 2014). For the years 2015 and 2016 cybersecurity becomes paramount to prevent another #Sonygate[1] (Solis, 2015). According to PWC (PWC, 2014) most enterprises are worried about the rise of cybercrime.

> *Cybercrime: Activities in which computers, telephones, cellular equipment, and other technological devices are used for illicit purposes such as fraud, theft, electronic vandalism, violating intellectual property rights, and breaking and entering into computer systems and networks (Speer, 2000).*

Cybercrimes are not different from regular crimes; the only difference is the use of internet while committing such crimes. Usually motive of cybercrimes can be found in self-enrichment. Since 2007 research shows that almost every enterprise experiences cybercrime while new methods do not seem to emerge fast (AIVD, GOVCERT.NL, KLPD, MIVD, 2010; GOVCERT.nl, 2007, 2008, 2009, NCSC, 2011, 2012, 2013, 2014). One of the most damaging threats are DDOS-attacks. DDOS attacks are detriment for companies, companies can experience loss of income, brand damage, loss of customer confidence and personnel costs (Dyn, 2014).

Cybercrime is a growing industry, the estimated costs to the global economy are between $375 to $575 billion (CSIS & McAfee, 2014). To prevent these cybercrimes, it is necessary to protect yourself with the use of solid cybersecurity measures to minimize the risk of successful cyberattacks. Cybersecurity and information security have a large shared denominator, but they do differentiate from each other. Wherein information security it is all about protecting data, cybersecurity focusses more on preventing and/or stopping cyberattacks.

[1] *#Sonygate seems to have been an inside job to get more attention (RT, 2014).*

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and enterprise and user's assets (ITU, 2008).

Enterprise and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. According to von Solms (2010) since the early 80's there have been 5 waves of information security. In the first wave information security was considered as a technological aspect. During the second wave, information security got managed by dedicated managers. The third wave considered the standardization aspect, comprehending best practices, compliance, and information awareness. Throughout the fourth wave, information security was considered as part of Corporate Governance. The fifth wave is the cybersecurity wave, concerning all internet based systems. As a result of this evolution are over a dozen frameworks with various degrees representing (parts of) each wave (Barlette & Fomin, 2010). These frameworks are complex, all embracing and ultimately costly to implement, resulting in the fact that only a minority of the SMEs seems to be using these frameworks (Patsis, 2007). Furthermore the existing frameworks are mainly designed on the behavior of large enterprises, without the giving attentions to unique characteristics that SMEs have (Dojkovski, Lichtenstein, & Warren, 2007).

As can be read in the ISO/IEC 27032:2012 there are besides the areas of information security and cybersecurity three other security areas, an overview is depicted in Figure 1. These areas are application security, network security and internet security. During this research, the focus is on cybersecurity management standards, including the latest management standards from the four previous waves in information security.

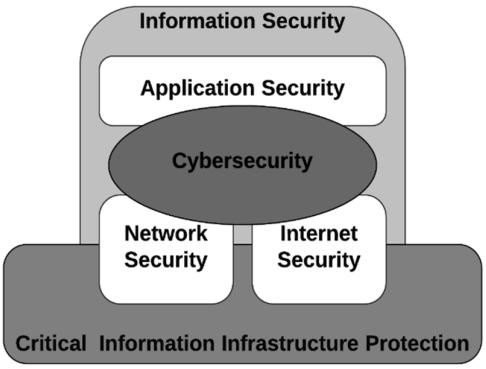

Figure 1 Relationship between cybersecurity and related domains (ISO/IEC 27032:2013)

Kindervag (2010) defines two cybersecurity philosophies, the first is the Trust but Verify and the second is Zero Trust. The Trust but Verify principle is widely used by enterprises and is based on a believe system that malicious individuals can't get past the heavily secured borders of IT Infrastructures, with the resulting effect that within these borders little to no security measures are implemented. On the other hand, within the Zero Trust principle, the whole IT Infrastructure is untrusted. Which means that all resources within the IT Infrastructure must be verified and secured, access controls must be limited and strictly enforced and network traffic must be logged and inspected.

To provide an overview of what has yet to come, in the proceeding enumeration states the chapters described in introduction:

1. Problem Statement;
2. Research Questions;
3. Relevance;
4. Research Model;
5. Systematic Literature Review;

6. Existing Maturity Model Analysis;
7. Define Objective Maturity Measurements;
8. Case studies;
9. Cooperation – ON2IT B.V.;
10. Challenges and Limitations;
11. Main Deliverables;
12. Deliverables.

1.1 Problem Statement

Making sure information is not compromised and your cyberenvironment is protected from potential threats will become more important for enterprises as they become more dependent from IT. With this increasing dependency of IT, enterprises should take measures that mitigate risks that emerge when IT is not-functioning or when the integrity of information can't be guaranteed. If enterprises ignore these risks, the resulting financial losses could be too much to bear for an enterprise in the case a disaster occurs or a cybercrime takes place.

> *"Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you."*
> *Theodore Roosevelt*

Especially SMEs often have often atypical IT environments and are often defenseless against certain risks (Dimopoulos, Furnell, Jennex, & Kritharas, 2004). When it comes to these risks, there are multiple issues that arise. For starters there is the problem of awareness, even if enterprises are aware of the risks they are not taking these areas serious enough (Bulgurcu et al., 2010). Once enterprises are aware of risks they will be needing continued training, because IT is growing steadily and new applications and security threads are emerging (Dhillon & Hentea, 2005). In case an enterprise would be aware about the threats it faces, they often have trouble making links in the complex relationships between relevant information security concepts (Fenz, Neubauer, Accorsi, & Koslowski, 2013). In reality it seems to be a fact that most enterprises have incomplete knowledge regarding information security in general (Fenz & Ekelhart, 2009). Especially SMEs live in the misconception that it is enough to install a firewall and antivirus to protect themselves against cybercrimes (Sangani & Vijayakumar, 2012). To prevent cybercrimes, continuous investments in cybersecurity measures and sophistical data protection systems are a must (Lewis, Louvieris, Abbott, Clewley, & Jones, 2014). Only this gives the problem of economics, how much should you spend on security (Carin, Cybenko, & Hughes, 2008).

Even though a lot of research has been done in the traditional Trust but Verify principle for cybersecurity (Denning, 2000; Moore, Ellison, & Linger, 2001; B. M. E. Whitman, 2003; B. Von Solms & Von Solms, 2004; R. Anderson & Moore, 2006; Ten, Manimaran, & Liu, 2010; Rabai, Jouini, Aissa, & Mili, 2012; Hahn, Ashok, Sridhar, & Govindarasu, 2013), there is not much research dedicated to cybersecurity with the Zero Trust principle in mind. The Trust but Verify principle assumes that it is impossible to pass the security borders of IT architectures for malicious individuals, which means that additional internal security measures are not necessary. Crucial principles of the Trust but Verify principle no longer hold, the border of the IT infrastructure does not end at the physical location of an enterprise, the inside of these borders are no longer a safe place for personal computers and enterprise software (Ward & Beyer, 2014). Not that long ago security and risk professionals where able to define the borders of security protection, these days the IT infrastructure has extended far beyond these borders which makes it much harder to lock down the borders (Balaouras, Kindervag, Holland, & Shey, 2014). In the current threat landscape the Trust but Verify has proven to be an ineffective way of securing the IT infrastructure, especially due to the exponential grow in mobile devices (Kindervag, Ferrara, Holland, & Shey, 2013). These days it is not enough to defend your IT Infrastructure to individuals, at the current date well-organized crime groups and nation-states are targeting the digital assets of enterprises. These entities have the ability to recruit insiders and are able to develop highly sophisticated attack methods, with these abilities they can easily pierce through heavily secured

borders (Kindervag, 2010b). Since history has shown that security borders can be broken, it is time for enterprises to change from Trust but Verify to the Zero Trust principle.

The Trust but Verify principle in security is widely used in enterprises, which means that cybersecurity measures are only taken at the borders of IT infrastructures. Notwithstanding these facts, only little research has been done regarding the Zero Trust principle. Especially since the complexity of networks keeps on increasing and network borders will slowly start to fade.

To summarize preceding argumentation, the problem statement used in this research is as following:

> *It is most important that enterprises start letting go of Trust but Verify and start embracing the Zero Trust principle. At the current date, the complexity of networks has increased exponentially. On top of that networks will keep extending well outside the controllable borders of enterprises. This means that these IT security borders will become uncontrollable if they are not already, without saying in time this will prone to disaster.*

The goal of this research is to create a scientific model which enterprises can use to improve their maturity in cybersecurity with the Zero Trust principle in mind, this model can also be used by enterprises starting with the implementation of the Zero Trust principle. According to my knowledge there has not been research done that explored possibilities in creating a model in the Zero Trust principle. This model will be created by combining two scientific methods for the creation of maturity models, these methods are the comparison analysis (Becker, Knackstedt, & Pöppelbuß, 2009) and focus area maturity modeling (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010). This research will gain insight in which security measures are necessary to fully implement the Zero Trust security principle in an IT infrastructures and research which dependencies these security measures have to define focus areas and maturity levels. Key challenges of this research will be finding measures in cybersecurity which fit in the Zero Trust principle and defining maturity levels in these measures. The result of these findings will be incorporated in a framework. Another interesting part will be the way in which enterprises comply to the Zero Trust principle. Enterprises should use this research to gain insight in ways to transform from Trust but Verify to Zero Trust, raise their maturity in Zero Trust and gain knowledge about Zero Trust cybersecurity measures.

1.2 RESEARCH QUESTIONS

To solve the problem statement described in chapter Problem Statement, this research uses one main research question. To answer the main research question, five sub-research questions are stated. The answers of the sub-research questions will be used to answer the main research question. When the main research question and sub-research questions are answered, it should be possible to create and validate the Zero Trust Maturity Model.

This research has the following Main Research Question:

> ***RQ:*** *In which manner can enterprises improve their cybersecurity maturity in the Zero Trust principle?*

To answer the main research question, the proceeding sub-research questions (SQ) are defined:

SQ1: *"What is known about cybersecurity related to the Zero Trust principle?"*

SQ2: "*Can existing cybersecurity (maturity) models be used in creation of a Zero Trust Maturity Model?"*

SQ3: "*Which focus areas and maturity levels need to be defined to create the Zero Trust Focus Area Maturity Model?"*

SQ4: "*Is it possible to measure objectively the maturity of enterprises in the Zero Trust Focus Area Maturity Model?"*

SQ5: *"Which controls have Dutch enterprises used to comply with cyber security in the Zero Trust principle?"*

SQ1 and SQ2 shall to a certain extent be answered via related literature that is going to be used in this research. The most defining sub-research question of these sub-research question is SQ1, SQ1 will reveal what aspects of information security are defining when using the Zero Trust principle. The answer of SQ1 is defining for the answer of SQ2, which is "*Can previous invented cybersecurity models be used in creation of a Zero Trust Maturity Model?"* This question is of big influence of the answer the remaining two sub-research questions. All-in-all SQ1 and SQ2 are going to provide solid insights regarding the Zero Trust principle.

Nonetheless, the lion's share of the research questions is answered via input from qualitative case studies held by clients of ON2IT. The focus of case studies is to gain insight in which manner enterprises can perform an assessment to define the Focus Area and Maturity of their Zero Trust principle implementation. To create a ZeTuMM it is if most important to research what the different focus areas are and which maturity levels there are to define. Several questions in the questionnaire are devoted to investigating in which manner enterprises assessed and improved their IT security.

Based on related literature the results of the case studies, a ZeTuMM will be created after answering SQ3 and SQ4. These questions are defined to create the base of the framework. The most difficult parts will be defining which measures enterprises can take for their IT infrastructure with the Zero Trust principle in mind and which measures each maturity comprehends. The results of SQ5 will be used to shape the steps between the maturity levels which the literature prescribes.

Another important aspect is that every type of enterprise should be able to use and apply the created framework, no matter what their business might be. So, a part of this research will be devoted to figure out a way to define certain profiles that define a categorization of enterprises. Based on these profiles, specific cybersecurity solutions will be prescribed in a maturity model that experts can use in order to assess and improve the current implementation of the IT security of enterprises with the Zero Trust principle in mind.

1.3 RELEVANCE

In the proceeding sections in this chapter the relevance of this research are elaborated. The following sections are described in this chapter:

1. Scientific Relevance;
2. Social Relevance.

SCIENTIFIC RELEVANCE

The main purpose is to create a framework that enterprises can use to assess their maturity in the Zero Trust principle. Zero Trust is a principle which has emerged in 2010, until now not a lot of research has been done in this subject. Mainly because enterprises seem to keep believing in the opposing Trust but Verify principle. There have only been a few enterprises who have embraced the Zero Trust principle and it will be highly interesting to compare the academic perspective to the practical implementation of enterprises.

Only a little bit of scientific research about the Zero Trust principle is available, this research will also aim to fill the gap between the literature and practical implementation at enterprises. Especially since it is not sure if some concepts which are written in the first paper about Zero Trust were suggestively described or at the time not yet available.

Moreover, this research will create a focus area maturity model which is partly based on existing (focus area) maturity models in the cybersecurity field. Thus, this research is going to give insight in the differences and overlaps between the two philosophies: Trust but Verify and Zero Trust.

SOCIAL RELEVANCE

Since people, enterprises and governments get more and more dependent on the functioning of IT. It is important that more research about cybersecurity should be executed. In some cases, IT saves lives by helping surgeons during surgeries, IT also helps with the logistics of our basic needs. In this digital information area in which we are living, IT needs to work 24/7, information needs to be integer and easily interchangeable. Especially the fact that information needs to be interchangeable comes with certain risks, information should only be seen by authorized entities and should not be manipulated while exchanged.

These days' news about hacks or security breaches are with some regularity in the news. There are various examples where people, companies or governments were hacked. And the problem is, it only seems to get worse as can be read in chapter Research Approach

This chapter will elaborate on the research approach of this thesis project. It starts with the description of the research model that will be used. Secondly, some information about the company that provides resources for this research is given. Furthermore, this chapter gives insights in which manner related literature search will be executed and how the quantitative research part will be executed. Lastly the challenges and limitations of this research are described.

1.4 RESEARCH MODEL

Depicted in Figure 2 is a quick overview of the stages that will be taken to execute this research. The steps represent a methodological approach which is used to solve the research questions stated in chapter Research Questions.

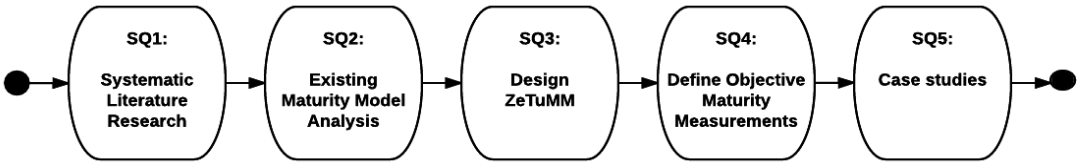

Figure 2 Research Model

In total, there are five stages defined in the used research model. The research starts with the execution of a Systematic Literature Research (SLR), during this step scientific guidelines are going to be used to perform a solid SLR. After completion of the SLR, the output will be used to conduct the Comparison Analysis of existing (focus area) maturity models in the field of cybersecurity. During the Comparison Analysis, existing (focus area) maturity models are reviewed. All the guidelines and security measures that comply with the Zero Trust principle will be extracted and used. This comparison analysis will be performed using following scientific guidelines. During the third stage, specific focus area will be defined and the first initial version of the Zero Trust Maturity Model (ZeTuMM) will be created. In the fourth stage objective maturity measurements, will be defined to calculate the maturity levels. During the Case Studies information about the realized implementation of the Zero Trust principle at Dutch enterprises will be gained.

1.5 Systematic Literature Review

To define, comprehend and use previously research about cybersecurity a Structured Literature Research (SLR) will be executed. The main research question and five sub-research questions, as stated in chapter Research Questions are used to successfully execute the SLR. Lessons learned from applying SLR to the software engineering domain will be used during the execution (Brereton et al., 2007).

Since the scope of this research is limited, it is of key importance that large amounts of previous research can be processed to harvest valuable pieces of information. A SLR is one of the solutions to do so, it is a specific process that researchers should follow to guarantee a high-quality review.

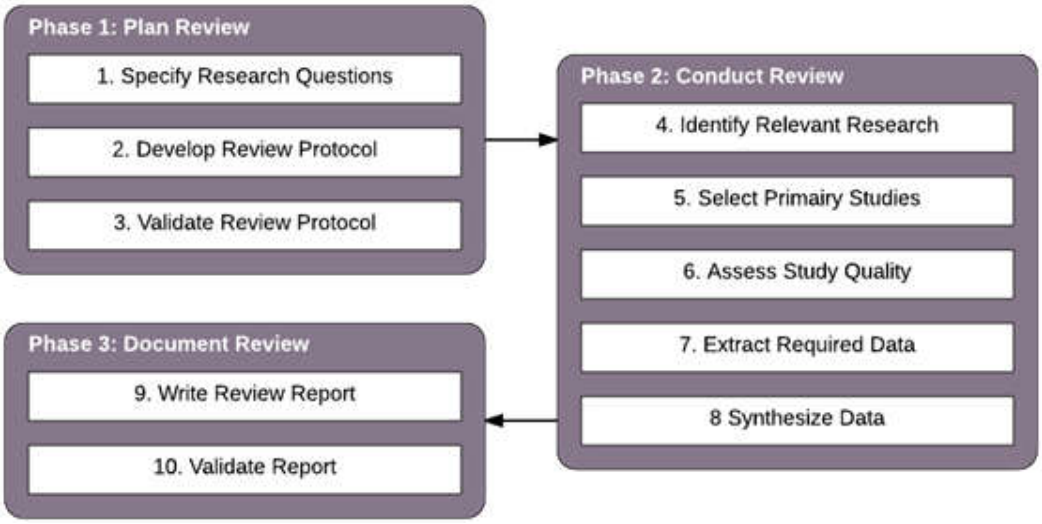

Figure 3 Systematic Literature Review (Brereton et al., 2007)

In total the SLR consists of ten activities which are classified in three phases. Figure 3 depicts the three phases. In the proceeding sections these phases and activities are elaborated. The Systematic Literature Review consists out of the following phases:

1. Plan Review;
2. Conduct Review;
3. Document Review.

Plan Review

During the first step, it is important that specific research questions are stated which should be answered. It is possible to change the research questions in the first phase. This is because the researcher will learn more about the subject during the research process and could learn new aspects that could change his perspective.

The second step is the creation of a Review Protocol. This is a protocol that should be used during the execution of the Systematic Literature Review. A review protocol should define the proceeding rules:

- Data sources;
- Search terms;
- Acceptance criteria;
- Extraction data form.

Throughout the third stage, the developed review protocol is tested whether the protocol gives a desired outcome. When the outcome of the review protocol is not satisfactory, the researcher should return to step two until the outcome is as desired.

Conduct Review

In step four the developed review protocol that is created in the first step is executed in various search engines. With the use of a spreadsheet a list of that contains related literature is recorded. This must be done by listing the titles of relevant papers which appear in the search results.

Step five begins when relevant research is identified. When the title of a paper is relevant to the research topic, the papers should be included in the spreadsheet. The researcher must read the abstract from the papers which are included in the remainder of the Structured Literature Research.

The sixth step is about assessing the quality of the remaining papers which are included after reading all the abstracts. Based on various pre-defined quality measures the included papers undergo a second inclusion/exclusion process.

Throughout step seven the specific (meta) data from the included papers are extracted. Extraction is executed via data forms which are designed in the second step.

During step eight, the extracted data from remaining papers is going to be synthesized within the sub-research questions.

Document Review

After completion of the Systematic Literature Review, the whole process and all the results are documented in the ninth step.

In the tenth step the document which is created should be validated by means of a review.

1.6 EXISTING MATURITY MODEL ANALYSIS

To compare existing maturity models, current cybersecurity (focus area) maturity models will be analyzed. This analysis will be executed by using the scientific approach described by Becker, Knackstedt, & Pöppelbuß (2009). This approach contains guidelines for the development of maturity models, which are defined in eight different activities. These eight activities are:

1. **Comparison with existing maturity models:** The need for the development of a new maturity model is substantiated by a comparison with existing models. The new model can be an improvement of an existing one. The ZeTuMM is created by looking to existing cybersecurity maturity models with the Zero Trust principle in mind.
2. **Iterative procedure:** Maturity models must be developed iteratively, i. e., step by step. It is important to develop the ZeTuMM iteratively. To ensure iterative development, information is gathered from various information sources, case studies and feedback from experts.
3. **Evaluation:** All principles and premises for the development of a maturity model, as well as usefulness, quality and effectiveness of the artifact, must be evaluated iteratively (for the problem of delimiting the evaluation criteria. This research is validated by means of case studies, based on resulting feedback gained from these case studies the ZeTuMM is improved.
4. **Multi-methodological procedure:** The development of maturity models employs a variety of research methods, the use of which needs to be well founded and finely attuned. This step will be guaranteed by using a systematic literature research, a comparison analysis, case studies and expert validation.
5. **Identification of problem relevance:** The relevance of the problem solution proposed by the projected maturity model for researchers and/or practitioners must be demonstrated. This document contains the chapter Relevance, this chapter describes the scientific relevance as well as the social relevance.
6. **Problem definition:** The prospective application domain of the maturity model, as well as the conditions for its application and the intended benefits, must be determined prior to design. With the use of this document and by answering the first sub-research question conditions and intended benefits will be determined.
7. **Targeted presentation of results:** The presentation of the maturity model must be targeted regarding the conditions of its application and the needs of its users. To make sure this maturity model suits all ranges of enterprises, the maturity model makes use of situational assessment criteria to define which focus an enterprise should take within the maturity model.
8. **Scientific documentation:** The design process of the maturity model needs to be documented in detail, considering each step of the process, the parties involved, the applied methods, and the results. The executed activities are going to be described extensively in resulting thesis and paper that will derive from this research.

After the completion of this research phase it will be determined which (parts of) existing (focus area) maturity models in the field of cybersecurity can be used in the creation of the Zero Trust Maturity Model.

1.7 Define Objective Maturity Measurements

To answer SQ4, additional literature research will be performed. The goal of this literatures study is to describe objective measurements to establish the maturity level of an enterprise. These objective measurements are an addition on the previous developed assessment instrument as described in step six from chapter Design Process ZeTuMM. These objective measurements should make the ZeTuMM more quantifiable.

1.8 Case studies

Qualitative research on state of Zero Trust principle will be executed with the use of semi-structured interviews. The goal of the case studies is to gain insight of the state of the practical Zero Trust principle implementations at Dutch enterprises and to validate the ZeTuMM. Feedback gained from these interviews will be used to improve the model. The interviews will take place at three case study enterprises in the Netherlands. Enterprises who are willing to participate were found using my network.

1.9 Cooperation – ON2IT B.V.

ON2IT is specialized in providing IT security services and solutions. They provide enterprises services and solutions which fit their IT-infrastructure, their grow perspectives and needs.

The company is driven by a passion for IT security. They help enterprises with the implementation of the right IT security solutions in their core network. They use knowledge and expertise as the base to offer enterprises a sophisticated and customized IT security strategy which suits their specific needs and requirements. To stay ahead of competition, they innovate and keep track of the newest trends and developments.

The company uses an Information Security Management System (ISMS), which is tested and approved by Lloyd's Register Quality Assurance per norms of information security (ISO/IEC 27001:2013). They use the international ISO codes of conduct as a framework for their policies regarding the IT security of confidential information. ISMS provides managed IT security products and services, offers 24/7 support and processes data for clients.

The company shares knowledge by providing publications, whitepapers, research, events and trainings. In this way, they offer enterprises clear guidance for smarter IT security. For students, they offer quality internships, provide trainings and give them the space to grow to the expert they want to become.

According to ON2IT, IT security is an organism which needs a constant focus. With the use of services, such as audits and consultancy, the company offers IT security that fits the needs and grow of enterprises. They help to improve IT security, minimalize business risks and secure valuable business processes. Along with services like implementation and project management they transform business strategy to concrete steps. They also offer highly customizable managed security services for a fixed amount per month.

1.10 Challenges and Limitations

The biggest challenge in the creation of the Zero Trust Maturity Model (ZeTuMM) will be the high diversity of enterprises. To define various focus areas, it is of importance to define certain profiles. Every enterprise is different and highly dynamic. Medium to large enterprises can consist of 50 to far over 250 employees and can operate in distinct sectors. This means it will be difficult to create a profile which will fit all types of enterprises. This profile is necessary to define which types of measures must be used to become cyber- and information secure in various maturity levels with the Zero Trust principle in mind.

The second challenge will be comparing and analyzing existing models. The goal of researching existing models is to find measures of cybersecurity that are in line with the Zero Trust principle. As previously mentioned current maturity models are created with the Trust but Verify in mind. With Trust but Verify only the borders of the IT infrastructure are secured instead of every entity in the IT-infrastructure. This could mean that a lot of aspects are not applicable within the Zero Trust principle. In various cases, it will probably be difficult to define whether certain measures in these models should be included within the ZeTuMM.

The third challenge will be to find enough enterprises who are willing to participate in these case studies. These case studies will go in-depth about the current state of cybersecurity and most enterprises are not eager to talk about their state of IT security.

This research will explicitly focus on creating the Zero Trust Maturity Model and will not research in the way enterprises should use and/or implement the model.

1.11 Main Deliverables

The results of this master thesis project will be documented in various deliverables. This chapter gives an overview of the main deliverables and a brief description.

Short proposal

The short proposal has already been written and is used as a basis for approval regarding a master thesis research project. Without saying this project has been approved by Utrecht University.

Long proposal

The short proposal is used as a basis for this document. The long proposal will act as the guideline for this master thesis project, it describes all important aspects about the research and in which manner it is conducted.

Master's thesis

The result of this research project is a master's thesis. This document will contain all important findings which are gained during this research. The thesis will at least conclude:

- Result Systematic Literature Review if related literature;
    - Including comparison analysis of existing maturity models;
- Result qualitative research regarding state of the Zero Trust principle;
- Zero Trust Maturity Model;
- Expert Validation of the Zero Trust Maturity Model.

Scientific paper

All the findings gained in this research and described in the thesis will be summarized in a scientific paper. If possible, this paper will be published in a suited journal.

Presentations

The results of this master's thesis research are presented. The first two presentations at the colloquium are to gain feedback about the results thus far. Once the thesis document is finalized, it will be presented at Utrecht University and ON2IT. To summarize, the following presentations will be held:

- Presentation at Colloquium;
- 2nd Presentation at Colloquium;
- Presentation at ON2IT B.V.;
- Defense at Utrecht University.

1.12 DELIVERABLES

The processes and deliverables are depicted in Figure 4. The schema is created by using process-deliverable diagram (PDD) (van de Weerd & Brinkkemper, 2008)

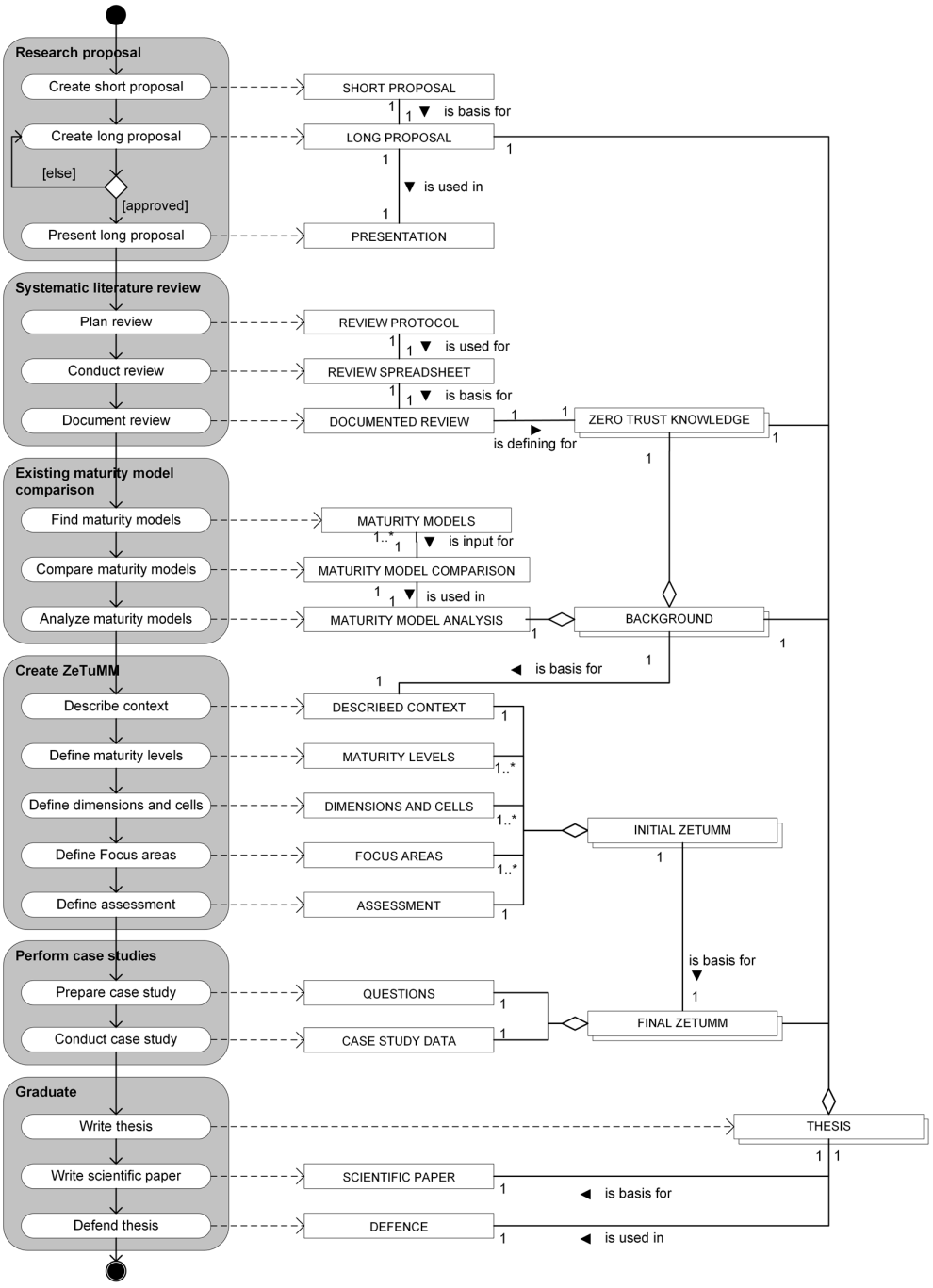

Figure 4 PDD Main Deliverables

Since the processes are already extensively described in chapter Research Approach, this document will not contain an activity table. As for the concept table, the main deliverables are described in chapter Main Deliverables.

2 Systematic Literature Review

This chapter describes the Systematic Literature Review that is performed during this master's thesis project. The aim of this SLR is to perform a structured review of published literature about cyber security, with the focus on maturity models or assessments. Another important part was reviewing the literature regarding the Zero Trust principle. The goal of this SLR is to answer SQ1, which is:

> *"What is known about cybersecurity related to the Zero Trust principle?"*

2.1 Previous SLRs

Standing on the shoulders of giants, it is obvious that various researchers have performed Structured Literature Reviews. This section describes previous SLRs that have been conducted in the field of cyber security.

A SLR from Braun et al. (2015) focused on previous applied mythologies on previous assessments of cybersecurity awareness. Relevant databases were searched with pre-defined keywords and the search was limited to papers from 2005 to 2014. In total, they identified 23 studies and extracted information included authors, publication year, used assessment method, target audiences, coverage of assessment and assessment goals. Previous research did not make use of the program evaluation technique for cybersecurity awareness assessments (Rahim, Hamid, Mat Kiah, Shamshirband, & Furnell, 2015).

Jansen (2014) conducted a SLR to learn more about risk assessments for hospitals regarding cyber- and information security. Electronic libraries were used to find research in two literature domains, the scope was limited to papers from 2009 to 2014. The SLR resulted in meta-data analysis of 36 relevant papers on qualitative synthesis and quantitative synthesis. Resulting on qualitative synthesis that explains retrieved concepts and research gaps, the quantitative synthesis provided methods and techniques from domain independent perspectives which apply to hospitals and health care. A clear research gap regarding a threat landscape for hospitals and quality factors for risk assessments where identified (Jansen, 2014).

Rebollo et al. (2012) executed a SLR of information security governance frameworks in the cloud computing environment. In total of six sources where used to search on six keywords. The paper does not mention the amount of papers that are identified, but the researchers have compared six frameworks on policies and processes adaption, control and audit, and Service Level Agreement (SLA). Current information security governance frameworks deal with most of the selected criteria, but some gaps must be filled in the development of future information security governance frameworks (Rebollo, Mellado, & Fernández-Medina, 2012).

Putri et al. (2011) performed a SLR to find identified security threats and attributes in the cloud to enhance information security in the cloud. In total six databases were searched for the first SLR with the goal to identify security threats in cloud computing and four databases where used for the second SLR to identify data about available frameworks for the development of security metrics. In total 82 (SLR1) and nine (SLR2) studies where selected as relevant. The study identified 41 SLA based information security metrics to assist clients as well as the cloud providers in covering security performance expectations and goals (Putri & Mganga, 2011).

Latif et al. (2014) conducted a SLR to categorize risks that are associated with the cloud computing, the scope for this study included risks that applied for the cloud service provider as well as the consumer. The researchers used eight digital repositories and selected full English papers from peer-reviewed articles that were published between 2009 and 2014. After following the SLR methodology the researchers identified 31 journal articles which were included. There are five main categories of risks related to cloud computing which involve both consumer as the cloud provider(Latif, Abbas, Assar, & Ali, 2014).

Xiao-yan et al. (2011) performed a SLR to define suiting measurement instrument parameters to determine the information security maturity of an enterprise. The researchers reviewed the maturity evaluation models Engineering-Capability SSE-CMM technology systems maturity model (ISO/IEC 21827), federal information security technology assessment framework (NIST) and control target management guidelines (COBIT) to create a new model which can improve the information security capability of an enterprise (Xiao-yan, Yu-qing, & Li-lei, 2011).

Iankoulova et al. (2012) used a SLR to provide a comprehensive and structured view of security requirements and solutions for cloud computing. The researchers have used Scopus as a source to search scientific literature. They only used conference papers and journal articles, published before the first quarter of 2011 and limited by subject area in computer science, engineering or business. After applying the criteria, they identified 55 relevant papers. A roadmap is provided which classifies nine security group requirements for researchers. Only little research has been done on the sub-areas non-repudiation, physical protection, recovery and prosecution and research which has been was on access control, integrity and auditability (Iankoulova & Daneva, 2012).

One of the more striking conclusions that can be made is that a lot of research has been done on cloud computing security. In the search for related SLRs, no single SLR was found with a topic focusing on (focus area) maturity models.

The results of the SLR are various frameworks, methods and assessments concerning IT security and risks when using cloud solutions, the results are not useful when a company want to improve their maturity in cybersecurity.

These SLRs point out a need for a SLR that will research cybersecurity, with the focus on maturity models or assessments and research related literature on the Zero Trust.

2.2 SLR Approach

The first step in performing a SLR is defining the research protocol. The protocol gives specifications in which manner the SLR is performed. With a proper definition of these specifications the SLR outcome is unbiased and these specifications also contributes to the rigorousness and traceability of this study. The research protocol that is maintained in the SLR exist of definitions for: Acceptance Criteria;

1. Search Terms;
2. Sources;
3. Data Extraction;
4. Test Protocol.

The proceeding paragraphs describes realizations of the executed SLR.

Search Terms

With the use of proper keywords the amount of relevant scientific literature narrowed down. It is of importance to select keywords that will harvest the scientific literature which is in scope and without disregarding important aspects. According to Duff (1996) it is best to use thesaurus and natural language searching during the execution of this search strategy. To ensure a comprehensive result of scientific literature the following keywords are used:

- Cybersecurity;
- Cyber Security;
- Information Security;
- Maturity Model;
- Gap Analysis;
- Assessment;
- Governance;
- Assurance.

Based on the selected keywords a logical statement is formulated. It is best to use a logical statement that comprehends and combines all the keywords. To gain more information about the Zero Trust principle, the following search statement is formulated:

SLRST1: *"Zero Trust" OR "Zero Trust Model of Information Security"*

During the comparison analysis, a secondary SLR needs to be performed. For this SLR the second search statement is formulated as:

SLRST2: *(Cybersecurity OR "Cyber security" OR "Information Security" AND ("Maturity Model" OR "Gap Analysis" OR `Framework OR Assessment OR Governance OR Assurance))*

SOURCES

Making sure the conducted SLR is rigor and unbiased, two search engines are used. These digital libraries are search engines with a general focus on scientific literature. These search engines are Google Scholar and Scopus.

ACCEPTANCE CRITERIA

To make sure the search statement results in a comprehensive set of relevant scientific literature, various criteria are given before reading through the results. Since the field of cyber security is fast developing, one of the criteria is regarding is to filter on literature from the past five years. Besides that, the Zero Trust Model of Information Security was firstly described in the year 2010, so it is expected not to find any papers regarding Zero Trust principle. Since the two search engines offer different criteria options, the following sections defines which criteria are to filter the search results.

Google Scholar

Within Google Scholar citations and patents are excluded from the search results

Scopus

In Scopus, the search statement is only executed in the Title, Abstract and Keywords.

DATA EXTRACTION

The goal of the data extraction is to harvest qualitative data from previous literature. Data that will be extracted is data regarding the Zero Trust principle and data regarding the corresponding cybersecurity maturity models which adhere to Zero Trust. During SLRST1 data regarding the Zero Trust principle will be extracted, this will be data regarding Zero Trust concepts, measures and architecture. For the SLRST2, data will be extracted that can be reused in the creation of the ZeTuMM, this will be data regarding maturity levels, focus areas, maturity assessments, etc. Data that is extracted is used to describe what is known about Zero Trust and compile a new and improved framework.

Since the SLR is focused on a qualitative review instead of a quantitative review, only a little metadata will be extracted from the papers. Some interesting metadata point will be what kind of article the paper is and from which country the paper originates.

TEST PROTOCOL

To test whether the search protocol provides a sufficient set of scientific literatures, the search statement and acceptance criteria are applied and tested in the search engines.

Test Results SLRST1

Table 1 depicts the test of search statement SLRST1 and acceptance criteria in the search engines.

Table 1 Test Results SLRST1

Source	Number of Articles
Google Scholar	About 273 results
Scopus	3 results
Total	276 results

276 results of a search statement are not much, but this is as expected. The Zero Trust Model of Information Security is first described in 2010 and only a few enterprises are using it nor are researchers researching it. Even though there are not that much results, Google Scholar and Scopus are both giving interesting results. So, the SLRST1 and the selected criteria will pass the test.

Test Results SLRST2

The results of applying the search statement SLRST2 and acceptance criteria in the search engines are depicted in Table 2.

Table 2 Test Results SLRST2

Source	Number of Articles
Google Scholar	About 16.900 results
Scopus	2.444 results
Total	19.344 results

A total of 19.344 records for the second search statement including acceptance criteria seems sufficient and comprehendible. After reviewing the first couple pages displaying search results, some interesting titles appeared. The SLRST2 as well as the associated acceptance criteria passed the test.

2.3 SLR HARVEST

Depicted in Figure 5 is the overview of the conducted SLRs. Because SLRST1 did not result in a significant dataset, 12 additional records were identified. These records were identified using literature from the ON2IT research repository and Google. The research repository from ON2IT provides various papers and reports about activities which ON2IT is involved in, this repository provided four additional references. With Google, the same SLRST1 - as described in chapter Search Terms - is used to search with Google. This resulted in eight additional references.

During SLRST2 the goal was to find various maturity models in scientific literature. The results are seven maturity models which have been identified and will be used in the comparison analysis. The comparison analysis is further described in chapter Maturity Model

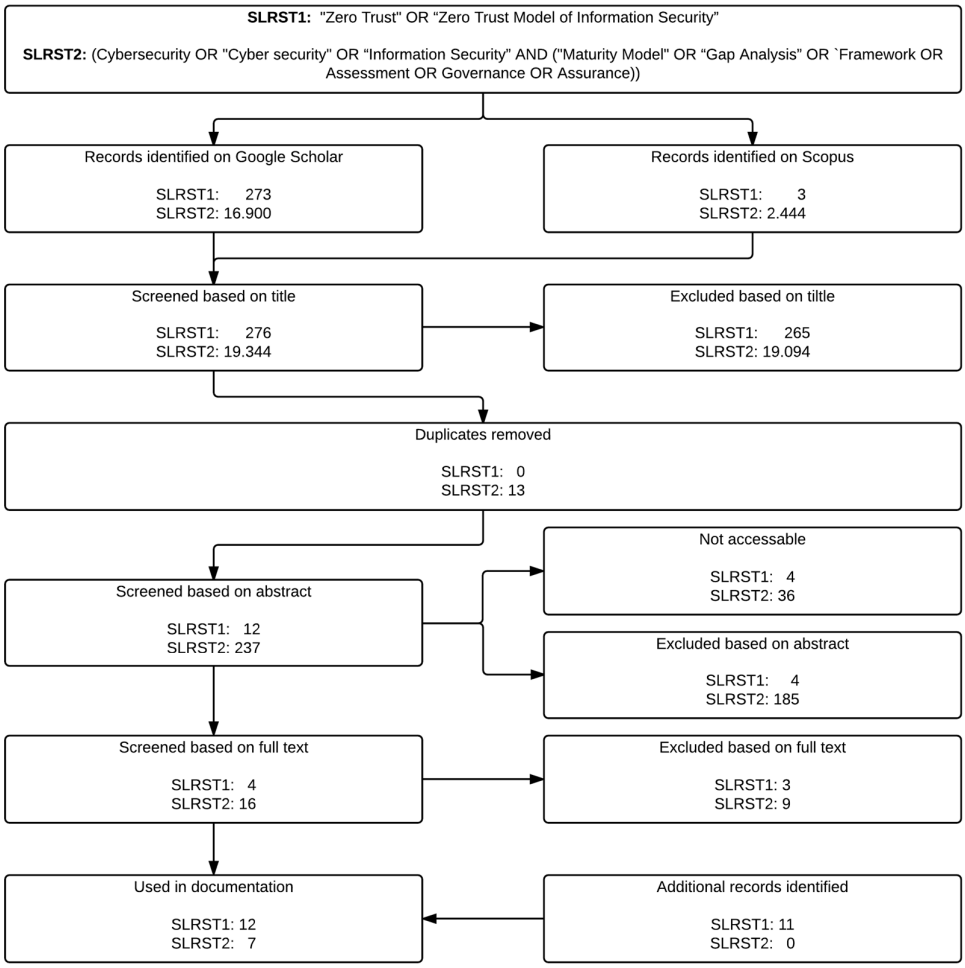

Figure 5 Overview of executed SLR

2.4 SLR Results

Both SLRST1 and SLRST2 are based on qualitative research, as opposed to quantitative research no literature analysis can be performed on the research results. So only the metadata of the selected papers will undergo literature analysis.

SLRST1

Literature that is used in the documentation of the SLRST1 is mostly based on Forrester Research, in total four of the 12 papers are published by Forrester. These four papers describes the Zero Trust Model of Information Security concept from John Kindervag. Another interesting paper that describes the Zero Trust principles and a technical implementation is from Google Research. Google Research has published a paper that is called BeyondCorp. BeyondCorp is Googles technical realization on the Zero Trust principle, the described realization is mostly on authentication and authorization. The remainder of the papers are further elaborations on the Zero Trust Model of Information Security.

SLRST2

After the completion of the SLRST2, seven different maturity models were identified. The subset of selected maturity models origin from various countries. Four of them were found using Google Scholar and the other three were found using Scopus. Five of the papers were presented at conferences and two were published in journals, so this means that the selected subset of maturity models have a high scientific value.

SLR Analysis

Depicted in Figure 6 is an overview of selected papers by year for SLRST1 and SLRST2. For SLRST1 the first two papers were written in 2010, after a couple years of silence some papers were written in 2013. In December 2013 at Lisa '13 Googler Synnot and Monsch announced that Google is adopting the Zero Trust principle, which could explain the larger amount of papers which were written in 2014. Most of the maturity models are published in 2011, there is no logical explanation to be found why this is the case.

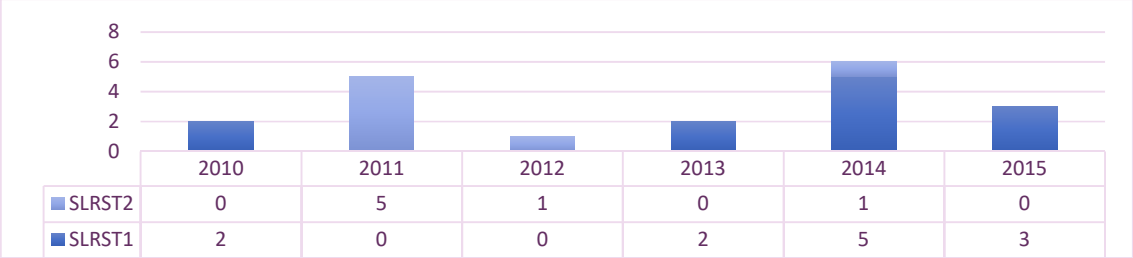

Figure 6 Overview of selected papers by year

Figure 7 displays the selected papers by type. As expected the SLRST1 yielded in only a few papers and thus additional references had to be searched via Google. With the use of Google four additional references have been found, three of them are reports and one is a workshop. The workshop consist of slides about a paper by (Kindervag, Balaouras, Holland, & Blackborow, 2015), which is from Forrester and is not freely accessible. The slides are presented by John Kindervag and is thus a good alternative

for the paper since it is not accessible. The scientific value of the SLRST2 is high, since the selected papers originate only from conferences and journals.

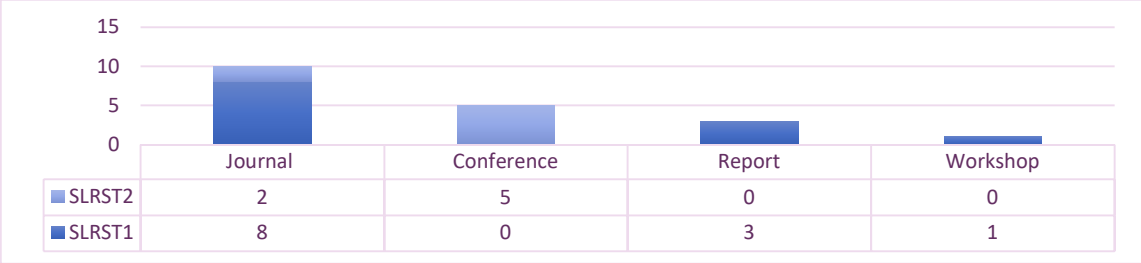

Figure 7 Overview of selected papers by type

The graph in Figure 8 displays the region of the selected papers. It is not surprisingly that the papers selected for SLRST1 mostly origin from the US. This is due to the fact that Forrester and Google are US-based companies and they published the majority of the papers. For SLRST2 the maturity models origin from various countries, which could imply there is a need for solid maturity models all over the world.

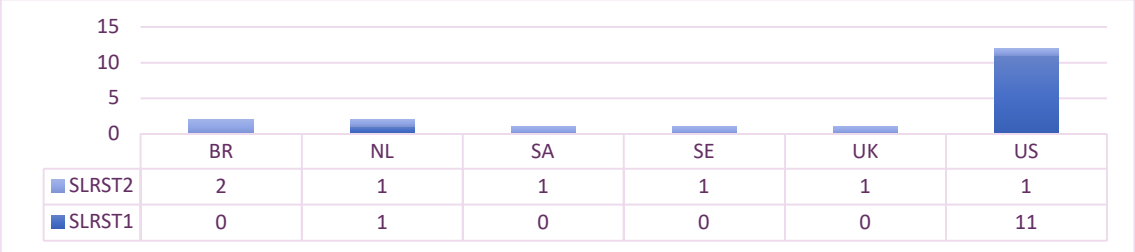

Figure 8 Overview of selected papers per region

2.5 SLR Documentation

During the synthetization and extraction phase of the SLR, the goal was to discover what is known about Zero Trust in the scientific literature. After reading the twelve papers, it seems that the Zero Trust principle makes a differentiation between concepts and measures. These concepts are abstract ideas which are required to realize a Zero Trust Infrastructure. Besides the three concepts, the papers mention various measures that are covered within the concepts. The three concepts of Zero Trust are:

- **Concept #1:** Ensure secure access to all resources within the network;
- **Concept #2:** Follow a least privilege approach and carry out strict access control;
- **Concept #3:** Log and inspect all traffic.

Table 3 depicts the overview of the synthesization results, the number of times a subject is mentioned in the selected papers and the amount of subject per paper. As can be concluded, the three Zero Trust concepts that are mentioned above are mentioned the most in the twelve papers. Respectively 'Concept #1' is mentioned nine times, 'Concept #2' is mentioned ten times and 'Concept #3' is mentioned eleven times. The other thirteen subjects are mentioned from one up to eight times.

Table 3 Overview of synthesization

	Subjects	(Kindervag, 2010a)	(Kindervag, 2010b)	(NIST, 2013)	(Scheerder, 2013)	(Ward & Beyer, 2014)	(Palo Alto, 2014)	(Banafa, 2014)	(Balaouras et al., 2014)	(Kindervag, Shey, & Mak, 2014)	(Kindervag et al., 2015)	(Palo Alto, 2015)	(Sivaraman, 2015)	**Times Mentioned**
C	Least Privilege & Access Control	x	x	x		x	x	x	x	x	x	x	x	11
C	Inspect & Log Traffic	x	x	x	x		x	x		x	x	x	x	10
C	Ensure Secure Access	x	x	x		x	x	x			x	x	x	9
M	Network Segmentation	x	x	x	x		x		x		x		x	8
M	Advanced Threat Protection						x	x	x	x		x	x	6
M	Application Whitelisting				x		x	x			x	x	x	6
M	Central Management		x	x			x		x				x	5
M	Data Abstraction								x		x		x	3
M	Control Shadow-IT							x	x	x				3
M	Incident Management							x	x	x				3
M	Securely Identifying Devices					x		x				x		3
M	Unprivileged network					x	x						x	3
M	Data Life-Cycle									x	x			2
M	Parallelize Switching Cores		x	x										2
M	Cloud Visibility									x				1
M	Inventory-Based Access Control					x								1
	Times mentioned	4	6	6	3	5	8	8	7	7	7	6	9	76

ZERO TRUST CONCEPTS

As previously mentioned, the Zero Trust concepts are abstract requirements for a Zero Trust network architecture. This section describes the three Zero Trust concepts, these concepts are:

1. Least Privilege & Access Control;
2. Inspect & Log All Traffic;
3. Ensure Secure Access.

LEAST PRIVILEGE & ACCESS CONTROL

The concept least privilege and access control is mentioned eleven times in the selected papers. It is the second main concepts as mentioned in the first paper about the Zero Trust Model of Information Security. The goal of this concept is to minimize the amount of resources and applications a user can access. Least Privilege& Access control ensures that users are only authorized to access resources and applications that they need to perform their work. On the one hand, in case a user account is compromised by cybercriminals or malware, this concept prevents that cybercriminals or the malware can move laterally within the network. On the other hand, it will prevent curious human beings accessing and potentially abusing data.

Kindervag (2010b) mentions two specific tools to manage Least Privilege & Access Control, these tools are Role-Based Access Control (RBAC) and Identity and Access Management (IAM) services.

INSPECT & LOG ALL TRAFFIC

Inspect and log all traffic is described as the third main concept in the first paper about the Zero Trust Model of Information Security. This concept is mentioned in total ten times in the selected papers. By inspecting and logging all traffic in real-time, abnormal user behavior and network traffic can be detected (Kindervag, 2010a). The goal of this concept is to detect breaches while they happen, it provides opportunities to adequately execute countermeasures to mitigate or stop the breach.

With the use of Network Analysis and Visibility (NAV) tools, all traffic should be logged and inspected (Kindervag et al., 2015). These NAV tools should be scalable and non-disruptive to the network. Examples of NAV tools are network discovery tools for finding and tracking assets, flow data analysis tools, malware detection, Security Information & Event Monitoring (SIEM) and user analytics.

By creating a Data Acquisition Network (DAN) all traffic should be intercepted and stored. This is the place where NAV tools should analyze the data, the result would be near real-time insight in the traffic that is passing through the network.

ENSURE SECURE ACCESS

Nine papers mention the concept of secure access to resources and applications within the network. It is the first main concept of the first papers about the Zero Trust Model of Information Security. By eliminating the trust in an internal network data will be protected in a similar way as data from the external network (Kindervag, 2010b). All traffic in the network must be assumed as a threat until proven otherwise. By using encrypted tunnels on the internal and external network, it is much harder for cybercriminals to intercept the data from the network.

By removing the trust from the network and applying policies, it should be defined whether and in which manner users or devices are authorized to access resources or applications.

ZERO TRUST MEASURES

This section described thirteen measures that have been harvested after reading the twelve papers that have been selected after performing the SLR. These measures all fit within the preceded mentioned concepts and are used as an example to make the abstract concepts of Zero Trust more concrete. The measures are sorted based on times mentioned in the papers as can be seen in preceding Table 3. This section describes the thirteen Zero Trust measures, these measures are:

1. Network Segmentation;
2. Advanced Threat Protection;
3. Application Whitelisting;
4. Central Management;
5. Data Abstraction;
6. Control Shadow IT;
7. Incident Management;
8. Securely Identifying Devices;
9. Unprivileged Network;
10. Data Life-Cycle;
11. Parallelized Switching Cores;
12. Cloud Visibility;
13. Inventory-Based Access Control.

NETWORK SEGMENTATION

The selected papers mention network segmentation eight times. Another widely used term in these papers for network segmentation is Microcore and Perimeter (MCAP). MCAP or Network segmentation is a concept where the network is divided in various smaller dedicated networks. These networks have their own purpose and should be created based on the type of data or applications that are hosted on that specific network segment (Palo Alto, 2014). The result is a minimum number of routes to network resources. This makes each network segments easily securable, because every network segment will have similar functionality and global policy attributes.

In the center of these network is a segmentation gateway stationed. A segmentation gateway creates secure network segments and provides functionalities of various security products like firewalls, Intrusion detection System (IDS), Web Application Filtering (WAP), network access control, content filtering, VPN gateways and other encryption utilities (NIST, 2013).

ADVANCED THREAT PROTECTION

A total of six papers mention the concept advanced threat protection. Advanced threat protection will detect exploits and malicious executables; it can detect known as well as unknown threats (Palo Alto, 2015). The solution is designed to detect a set of core techniques that attackers use to infiltrate a network and block them on detection before any kind of damage is done.

Advanced threat protection can be classified as a combination of anti-virus, anti-malware, intrusion prevention, sandboxing, anti-phishing, DDoS mitigation services and advanced threat prevention technologies.

APPLICATION WHITELISTING

Application whitelisting is mentioned in six papers. Application whitelisting is a technique that stops unauthorized and malicious applications from running on servers and personal computers. The goal is to guarantee that only selected applications and software libraries (DLLs) can run on an operating system and that all other applications and DLLs are blocked (Sivaraman, 2015). While the primary goal of this measure is to prevent malware from spreading, it also prevents the installation and use of unauthorized applications.

There are various applications and features within OS available that let you whitelist applications.

CENTRAL MANAGEMENT

The selected papers mention the measure centrally managed five times. With the segmentation gateway at the center of your network, the switches should be located around the center of the network and security professionals should maintain controls on a massive central managed backplane (NIST, 2013). The decentralization of these switches it makes it difficult and time consuming to manage these separately. The goal of this concept is to manage all network switching elements by a single central managed network backplane.

Various vendors offer solutions to centrally manage the switches within the network. When there is a high diversity of switches it could be that specialized software must be bought to control all those types.

DATA ABSTRACTION

The measure of data abstraction is mentioned three times in the papers. Data is only valuable for cybercriminals if they can access it. By abstracting data that is stored within the IT infrastructure network resources, it will be more difficult to access the data in the case it is exfiltrated by cybercriminals. Besides abstracting the data, the connection between servers and clients and connection to the cloud should also be abstracted (Sivaraman, 2015). This prevents that attackers can capture data when they intercept a connection.

For abstraction purposes, various techniques that can be used. These abstraction techniques are encryption, tokenization and masking.

CONTROL SHADOW IT

Three papers mention the subject of control shadow IT. Shadow IT is a term used to define unsupported software and hardware that is used within the network. When shadow IT is used within the network it will mean that there are no measures to mitigate potential risks. Thus, shadow IT will lead to greater security threats and risks for enterprises, because the IT department of an enterprise does know about the existence of these hardware or software.

To control the use of shadow IT, the IT department should have adequate processes that support, guides and advices business units within an enterprise in how IT can best support their processes (Banafa, 2014).

INCIDENT MANAGEMENT

Incident management is mentioned three times in the selected papers. Incident management helps to prevent security incidents by detecting, prioritizing and addressing vulnerabilities in the IT infrastructure of an enterprises (Balaouras et al., 2014). Security incidents will occur over time and it is of importance to have a solid incident response plan designed before security incidents happen.

Without proper incident response, it will be difficult to stop or contain a security incident and have proper forensic evidence to investigate incidents or restore the service after compromises.

SECURELY IDENTIFYING DEVICES

The selected papers mention securely identify the device three times. Before a user can connect to a resource within the network, the device should be identified (Ward & Beyer, 2014). By creating an inventory database, devices within the network can be referenced to records in that database. When a device is not matched with a record within the inventory database, the device should not be able to connect to any resources within the IT infrastructure.

By implementing an inventory database and keeping track of the lifecycle of the device, it is possible to monitor and analyze the state of the device. With the use of device certificates and a device qualification process each device can be securely identified.

Before a device can receive a device certificate the state of the device should be checked whether it is up to date and not compromised by any kind of malware. This device certificate should be renewed occasionally to enforce the state of security.

UNPRIVILEGED NETWORK

The subject of an unprivileged network is mentioned three times in the papers. This measure removes the trust from the internal network and prevents that attackers can move laterally within the network (Palo Alto, 2014). Within this network only internet, limited infrastructure services and configuration management services should be available.

A RADIUS server should be implemented that can assign devices on to a network based on an 802.1x handshake authentication. When devices connect to this network, wired as well as wireless access, it should be defined whether the device is a managed device that can access the IT infrastructure or if it's an unrecognized device that can only access the guest network (Ward & Beyer, 2014).

DATA LIFE-CYCLE

Data life-cycle is a subject that is mentioned in two of the selected papers. Data life-cycle an approach that locates and indexes data that are generated by users. After the data is identified it should be subject to a data classification process. When data is properly classified it makes it more achievable to take appropriate measures to protect that data (Kindervag et al., 2014). Not all data that an enterprise generates is valuable for attacker and thus must be protected with the best measures available. When enterprises correctly classify data, specific security measures and protocols can be taken so that data is securely processed.

There are certain types of data that a subjected to regulatory compliance purposes, these regulations are mostly for personal identifiable information. These regulations specify how those types of data should be protected. The IT infrastructure should be configured according to these regulations.

PARALLELIZED SWITCHING CORES

Parallelized switching cores is a measure that is mentioned twice in the selected papers. In contrary to the Trust but Verify security approach, where all the switches of the network are placed on the backplane of a network, the Zero Trust approach mandates that the switches are placed around the segmentation gateway (Kindervag, 2010a).

With the use of previously mentioned 'Centrally Managed' measure, these parallelized switches should be managed in a central manner.

CLOUD VISIBILITY

The concept of cloud visibility is mentioned one time in the selected papers. Cloud visibility is getting insight in the type of cloud services that are used within enterprises (Kindervag et al., 2014). Nowadays there are many cloud services available and it is not always clear to enterprises where their data is stored. To protect the data and get insight in where it is stored, an enterprise can get control over their data. This will result in less data loss or data leakage.

Various vendors offer solution to get insight in the types of cloud services that are used in your enterprise. These solutions can provide insight in where and which types of data sets are stored.

INVENTORY-BASED ACCESS CONTROL

One paper mentions the concept of Inventory-based access control. This measure defines that various levels of trust are given to users based on the type and state of a device. When a user has a device that is not up to date, uses a specific location or users a phone or a tablet it should be that a user cannot access every resource within the network (Ward & Beyer, 2014). When a user does want to access those resources, the user should be asked for extra authentication measures or that the device should be updated first.

With the use of an access control engine, various levels of trust can be given to users. The access control engine defines which parts of the IT infrastructure can be accessed and based on what type of authentications methods.

2.6 ZERO TRUST NETWORK ARCHITECTURE

The main difference between a Zero Trust network architecture and trust-but-verify network architecture is the way in which the network is designed. With a Trust but Verify network all network resources are placed in the core of the network as can be seen in Figure 9.

All resources within network can be entered via the enterprise network (distribution layer) and the internet (Edge layer). All the security measures used in this network design, stated in Table 4, like Firewall (FW), Digital Asset Management (DAM), Database Encryption (DB ENC), Data Leak Prevention (DLP), Intrusion Prevention System (IPS), Network Access Control (NAC), Virtual Private Network (VPN), Web Application Firewall (WAF), Web Content Filtering (WCF) and Wireless Local Network Gateway (WLAN GE) are all embedded in the core of the network with separated systems.

All network resources are accessed via this single layer of security. Once a malicious attacker has breached this singles security layer, the malicious attacker owns all resources. As more and more functionalities are added to corporate networks, securing all network traffic has become an – near to impossible – task for security professionals.

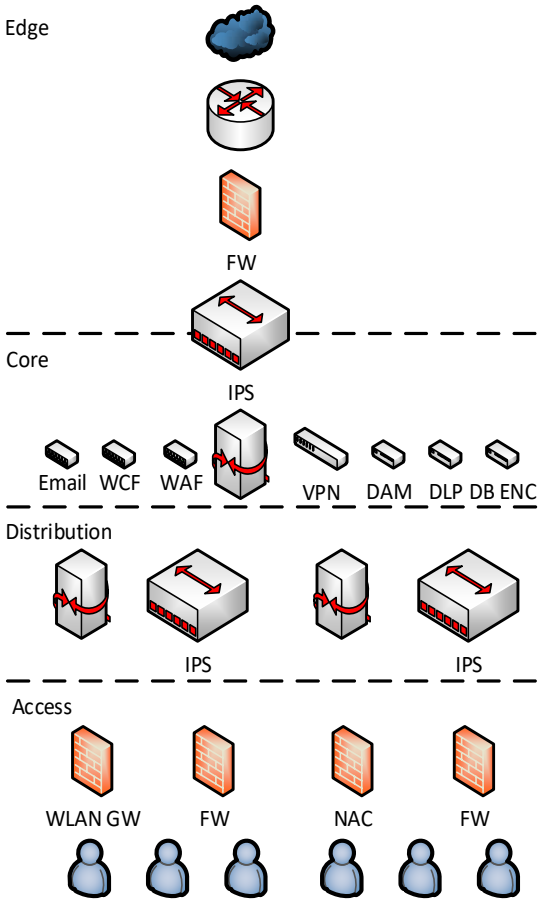

Figure 9 Trust but Verify Network Architecture (Kindervag, 2010a)

Table 4 Legend Trust but Verify Network Architecture

Abbr.	Meaning	Abbr.	Meaning
FW	Firewall	NAC	Network Access Control
DAM	Digital Asset Management	VPN	Virtual Private Network
DB ENC	Database Encryption	WAF	Web Application Firewall
DLP	Data Leak Prevention	WCF	Web Content Filtering
IPS	Intrusion Prevention System	WLAN GW	Wireless Local Area Network Gateway

Figure 10 provides a graphic scheme regarding the Zero Trust network architecture. This network is secured by means of Network Segmentation (Microcore and Perimeter (MCAP). Every resource with a specific functionality has been grouped in segments. This makes it much easier to control the network traffic to and from that specific network segment.

In the center of the network a Segmentation Gateway is placed to direct network traffic to destined network segments. Not only redirects the Segmentation Gateway traffic to a specific network segment, the Segmentation Gateway also functions as cryptographic control, monitors activity, filters content, firewall, intrusion prevention system and access control.

The Wireless network segment (WL MCAP) host the RADIUS server that assigns devices on the right network based on an 802.1x handshake authentication. The User network segment (User MCAP) hosts the domain controller and all domain accounts on a separate network. The Database (DB MCAP) and Application network segment (APPS) contain databases and applications with similar functionality. Since Card Holder Data (CHD) is more sensitive data compared to average company data, the CHD has a specific network segment what can be better secured. The World Wide Web network segment (WWW MCAP) is more sensitive for external attacks, and thus has an extra Web Application Firewall in front of that network segment.

The parallelized switching core that is necessary to maintain a Zero Trust network are managed with the Management Server (MGMT Server). To Inspect and log all traffic within the network, system that inspect and log all traffic are grouped in a Data Acquisition Network (DAN). With the use of Security information and Event Monitoring (SIEM) and Network Analyze and Visibility solutions a near real time view of the network traffic can be generated to detect anomalies.

Table 5 depicts the legend. Not all subjects that are mentioned in Table 3 are depicted in the drawing, this is because not all subjects are part of the network architecture or that a concept is part of another attribute within the network architecture.

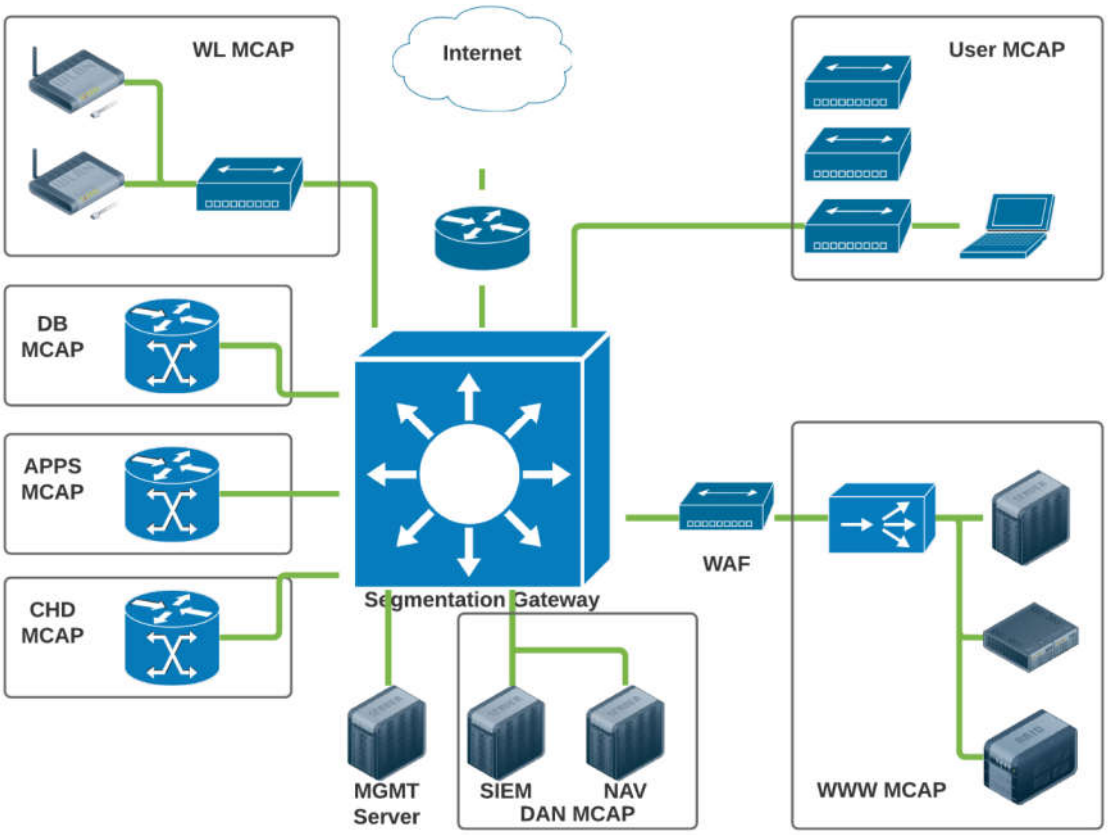

Figure 10 Zero Trust Network Architecture (Kindervag, 2010a)

Table 5 Legend Zero Trust Network Architecture (Kindervag, 2010a)

Abbr.	Meaning	Abbr.	Meaning
APPS	Applications	NAV	Network Analysis and Visibility
CHD	Cardholder Data	SIEM	Security Information and Event Management
DAN	Data Acquisition Network	User	User account
DB	Database	WAF	Web Application Filtering
MCAP	Microcore and Perimeter	WL	Wireless
MGMT	Management	WWW	World Wide Web

3 Maturity Model Analysis

This chapter describes the maturity model comparison study which is performed during this thesis. The maturity model comparison study is part of the maturity model development approach as described by (Becker et al., 2009). The goal of the comparison study is to validate whether parts of existing maturity models comply with the Zero Trust principles, and thus should be reused in the creation of the ZeTuMM. This chapter describes:

1. Identified Maturity Models;
2. Conclusion.

3.1 Identified Maturity Models

The maturity models have been identified with the use of scientific search engines Google Scholar and Scopus. After completion of the SLR, with the use of the SLRST2, a total of seven maturity models have been identified. The Identified maturity models are depicted in Table 6.

Table 6 Identified Maturity Models

Maturity Model	Author	Year	Source	Type	Ori.
Five Stage to Information Security (5S2IS)	(Gillies, 2011)	2011	Scholar	Journal	UK
Information Security Maturity Model (ISMM)	(Saleh, 2011)	2011	Scholar	Journal	SA
Community Cyber Security Maturity Model (CCSMM)	(White, 2011)	2011	Scholar	Conference	US
(e-Government) Information Security Maturity Model (ISMM)	(Karokola et al., 2011)	2011	Scholar	Conference	SE
GAIA Maturity Level Information Security (GAIA-MLIS)	(Coelho, Jr, Lemes, & Jr, 2014)	2011	Scopus	Conference	BR
(Case Study) Information Security Maturity Model (ISMM)	(Silva, Paula Costa, Poleto, & Moura, 2012)	2012	Scopus	Conference	BR
Information Security Focus Area Maturity Model (ISFAM)	(Spruit & Roeling, 2014)	2014	Scopus	Conference	NL

Identified maturity models will be compared and to the Zero Trust principles as defined in chapter SLR Documentation. The goal of the comparison study is to extract useful elements from already existing maturity models that can be reused for the creation of the ZeTuMM. The models will be compared on:

- Introduction;
- Foundation;
- Maturity Construction;
- Domain Construction;
- Strengths.

FIVE STAGE TO INFORMATION SECURITY (5S2IS)

The 5S2IS (Gillies, 2011), depicted in Figure 11, has been developed to implement efficient and competent information security management at SMEs, even if they have do not aim to become certified. With the use of the 5S2IS, companies can choose which measures they implement to mitigate risks to an acceptable level.

	Security Policy	Organizing Information Security	Asset Management	Human Resources Security	Physical and Environmental Security	Communications and Operations Management	Access Control	Information Systems Acquisition	Development and Maintenance	Information Security Incident Management	Business Continuity Management	Compliance
1: Commitment												
2: Systematic												
3: Monitored												
4: Improving												
5: Embedded												

Figure 11 Five Stage to Information Security

FOUNDATION

ISO27001, ISO27002 and the Capability Maturity Model (Humphrey, 1989) are the foundations which are used as a foundation for the 5S2IS.

MATURITY CONSTRUCTION

5S2IS makes use of 5 maturity levels. **Level 1: Commitment;** during this stage key performance indicators (KPIs) are defined. **Level 2: Systematic;** protocols and processes are defined to accomplish the pre-determined KPIs. **Level 3: Monitored;** outputs of protocols and processes are measured against the KPIs. **Level 4: Improving;** measurements of the KPIs are used to identify and improve shortcomings in the processes and protocols. **Level 5: Embedded;** the enterprise improves continuously and could choose for certification.

DOMAIN CONSTRUCTION

In total, the 5S2IS has 11 domains. These domains are based on the code of conduct extracted from the ISO27002:2005. These domains are depicted in Figure 11.

STRENGTHS

The 5S2IS is a high-level overview of crucial domains within information security. With the use of a stepwise approach to implement information security measures, the maturity model is easily approachable for enterprises. The author suggest the creation of a computer-based tool to reduce further obstacles by reducing the impact and investments when implementing the information security domains.

INFORMATION SECURITY MATURITY MODEL (ISMM)

Figure 12 depicts the ISMM (Saleh, 2011). The purpose of this maturity model is to give enterprises the ability to measure the state of their implemented information security practices. The ISMM should be used as a process that manages, measures and controls the information security management practices.

Combined Assessment	Starts	Compliance Level
0 – 1.5	One star	None Compliance
1.6 – 2.5	Two star	Initial Compliance
2.6 – 3.5	Three star	Basic Compliance
3.6 – 4.5	Four star	Acceptable Compliance
Above 4.6	Five Stars	Full Compliance
Overall Rating and Compliance Levels		

Figure 12 Information Security Maturity Model (Saleh, 2011)

FOUNDATION

The author does not mention exactly what the foundation is of the ISMM. The paper does mention four high level domains, which are corporate governance, system architecture, service management and enterprise culture. But the author only maps COBIT on Corporate Governance and TOGAF on system architecture.

MATURITY CONSTRUCTION

The ISMM has five levels of compliance. **Level 1: None Compliance;** which means that an enterprise has non-existing policies and procedures regarding information security. **Level 2: Initial Compliance;** within this stage an enterprise is aware about the risks they face, but the state is characterized by being chaotic, inconsistent, ad hoc and responsive. **Level 3: Basic Compliance;** procedures and processes are informal defined, core business activities and systems are protected. **Level 4: Acceptable Compliance;** all information security management policies and protocols are centrally managed. **Level 5: Full Compliance;** an enterprise is aware about the risks it faces and every information security need from the business is monitored and improved.

DOMAIN CONSTRUCTION

Every domain within the maturity model is outlined as a question in a corresponding questionnaire, these questions are about measures for people, information, systems and networks. The questionnaire makes use of the four high level domains, which are corporate governance, system architecture, service management and enterprise culture. These four high level domains have ten sub-domains. In total, there are 99 questions defined, the questions do not include any capabilities and are highly subjective. The questions should be answered by yes or no and must be rated between zero to five stars.

STRENGTHS

ISMM is a low-level overview of information security that provides various measures for information security. With the use of four high-level domains, the maturity model takes in account the corporate governance, system architecture, service management and enterprise culture and provides corresponding security measures. The model provides a wide range of detailed measures and enterprises can decide whether they deem certain measures necessary.

COMMUNITY CYBER SECURITY MATURITY MODEL (CCSMM)

Depicted in Figure 13 is the CCSMM (White, 2011), it is developed to assist enterprises, communities and states in creating their own cybersecurity programs to increase awareness about potential cyberrisks. The goal of the CCSMM is to give communities means to further develop and improve these programs. The maturity model provides three tools that should be used to evaluate and improve cyber security practices. It provides a 'yardstick', this yardstick is used to measure the state of cybersecurity and maturity level, a 'roadmap' is provided to improve the community's state of cyber security and a common reference point and terminology are provided for the members to exchange best practices and experiences.

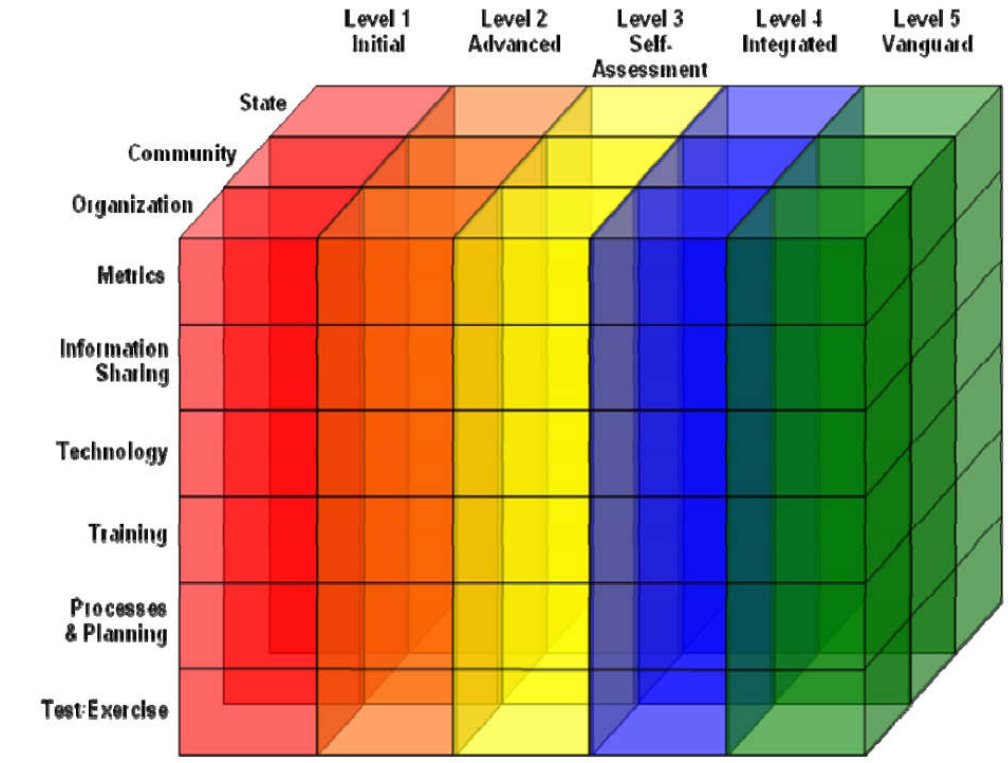

Figure 13 Community Cyber Security Maturity Model (White, 2011)

FOUNDATION

The author does not explicitly state what the foundation is of the CCSMM. A footnote in the paper reveals that the Cyber Security Division Department of Homeland security has funded the implementation in 5 different states in the USA.

MATURITY CONSTRUCTION

The CCSMM has five levels of maturity. **Level 1: Initial;** this stage has minimal cybersecurity awareness, collaborations and evaluations. **Level 2: Advanced;** there is cybersecurity awareness among the leaders, some collaboration within the community and initial evaluation of policies and procedures are started. **Level 3: Self Awareness;** cybersecurity awareness programs are promoted for enterprises by the community leaders, there is formal local collaboration in the community, cybersecurity exercises are held and policies and procedures are evaluated. **Level 4: Integrated;** cybersecurity awareness programs are promoted for citizens by leaders and enterprises, formal information sharing and analysis to community and autonomous cybersecurity exercises are held with real data/assessments. **Level 5: Vanguard;** awareness is community imperative, fully integrated security operations center for community and full-scale cybersecurity exercises and involve and/or mentor other communities.

DOMAIN CONSTRUCTION

As can be seen in Figure 13, the CCSMM has three dimensions. The first dimension is the five levels of maturity. The second dimension is regarding various entities that should be included, which are State, Community and Enterprise. The third dimension is about the domains: Awareness, Information Sharing, Technology, Training, Process & Planning and Test Exercise.

STRENGTHS

The CCSMM is a high-level overview of cybersecurity. It is a tool that communities can use to measure and improve their preparedness when it comes to cyberattacks, this is accomplished by taking in account the various entities that play a role. The best quality of the CCSMM is the domain of information sharing between the various entities and the human aspect of cybersecurity, which is awareness. Another quality within the CCSMM is the cybersecurity exercises.

(E-GOVERNMENT) INFORMATION SECURITY MATURITY MODEL (ISMM)

Figure 14 represents the (e-Government) ISMM (Karokola et al., 2011). The model is developed to measure the maturity of technical and socio/non-technical domains within the information security practices. The model is created for enterprises who provide secure government services. By using this model enterprises can measure maturity of their information security practices. With the measurement results, they are also able to create concrete plans to improve implementations and controls of their technical and socio/non-technical domains. In contrary to previously developed ISMMs for digital government services, this model measures both the quantity and quality of the government services.

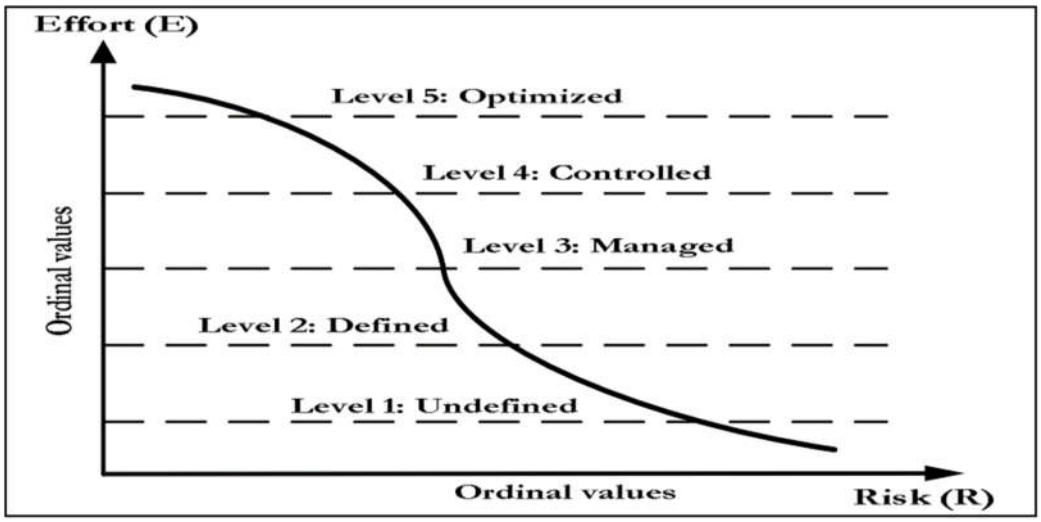

Figure 14 (e-Government) Information Security Maturity Model levels, Risk vs Efforts (Karokola et al., 2011)

FOUNDATION

Before this model was created, the researchers performed a comparison study where they compared eight maturity models. Based on three categories (management, evaluation and awareness) they selected the best fitting maturity model. The selected models ISM3 (Consortium, 2007), PRISMA (Bowen & Kissel, 2007) and GISMM (Dzazali, Sulaiman, & Zolait, 2009) are the foundation for the ISMM.

MATURITY CONSTRUCTION

The ISM3 has five maturity levels. **Level 1: Undefined;** enterprises have low Information Security Targets (IST), operates in low security risk environment (SRE), policies and process matrixes are not compulsory, some risk reduction processes and awareness is compulsory. **Level 2: Defined;** enterprises have normal IST, operates in normal SRE, process matrix not mandatory, security policies are defined, reactive security risk reduction and information security is in place. **Level 3: Managed;** enterprises have high IST, operate in high SRE, highest security risk reduction, process matrix are not mandatory and security policies are in place. **Level 4: Controlled;** enterprises have higher IST, operates in higher SRE, highest risk reduction, use of process metrics are obligated, information security is embedded and security policies are in place. **Level 5: Optimized**; enterprises have higher IST, operates in highest SRE, highest security risk reduction, process metrics are obligated, information security embedded and security policies are in place.

DOMAIN CONSTRUCTION

The ISM3 makes use of seven domains, these domains are Hardware Solutions, Software Solutions, Ethical & Cultural, Legal & Contractual, Administrative & Managerial, Operational & Procedural and Awareness.

STRENGTHS

One of the stronger elements within this maturity model is that measures for the domains are focused around the three categories management, evaluation and awareness. Another reusable aspect is the scientific calculation that is used to calculate the security risks and security exposures.

GAIA MATURITY LEVEL INFORMATION SECURITY (GAIA-MLIS)

The goal of the GAIA-MLIS (Coelho et al., 2014)is to provide enterprises insight in their maturity level in information security system, this is done by giving insight in their strengths and weaknesses. Based on the state of an enterprise the model gives concrete advice on how they can improve their information security practices. Its objective is to determine weaknesses and help with the improvement in the management of one of the five areas which are depicted in Figure 15.

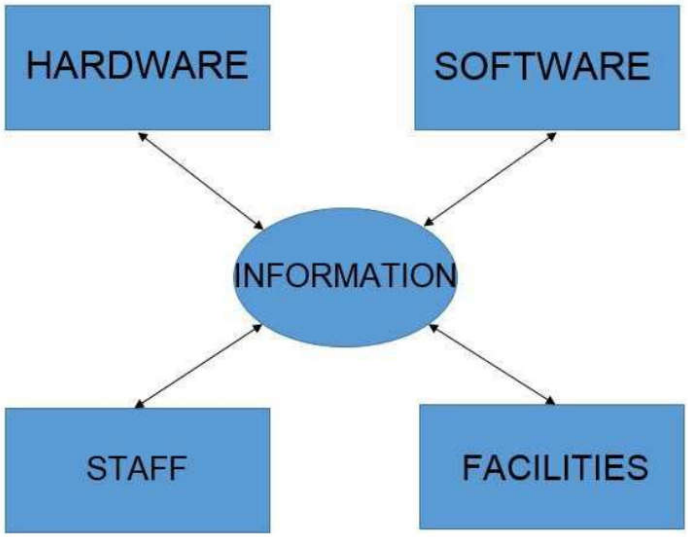

Figure 15 Relationship areas GAIA Maturity Level Information Security (Coelho et al., 2014)

FOUNDATION

Standards from the COBIT 5 (ISACA, 2012), ISO27001:2005 (ISO, 2005a) and ISO27002:2005 (ISO, 2005b) are the foundations for the GAIA-MLIS.

MATURITY CONSTRUCTION

GAIA-MLIS makes use of five maturity levels. **Level 0: No Insurance;** processes and policies are not defined, no awareness, no consequences after security incident, no IAM, no access control, physical facilities are not secured, equipment not protected against external threats, lack of network management, assets data is not encrypted, asset inventories are not identified and there is no data classification. **Level 1: Entry Level Insurance;** some processes and policies are defined, no awareness, no consequences after security incident, some IAM, no access control, physical facilities are not secured, some equipment is protected against external threats, basic network management, assets data is not encrypted, asset inventories are not identified and there is no data classification. **level 2; Regular Insurance**; processes and policies are defined, some awareness, no consequences after security incident, IAM, some access control, physical facilities are not secured, some equipment is protected against external threats, basic network management, assets data is not encrypted, asset inventories are identified and there is no data classification. **Level 3: Partially Safe;** processes and policies are defined, awareness programs, consequences after security incident, documented IAM, access control, physical facilities are secured, some equipment is protected against external threats, efficient network management, assets data is encrypted, asset inventories are identified and there is data classification. **Level 4: Fully Insured;** processes and policies are defined, awareness programs,

consequences after security incident, documented IAM, access control, physical facilities are secured, equipment is protected against external threats, efficient network management, assets data is encrypted, asset inventories are identified and there is data classification

DOMAIN CONSTRUCTION

The GAIA-MLIS makes use of 5 domains, these domains are Hardware, Software, Facilities, Staff and Information.

STRENGTHS

The domains that the GAIA-MLIS identifies covers every aspect of an enterprise. The maturity level construction – starting with 0 – could also be an interesting approach to start measuring the maturity in the ZeTuMM. The author uses a graphical representation, which gives a solid overview of the maturity level an enterprise has.

(CASE STUDY) INFORMATION SECURITY MATURITY MODEL (ISMM)

Depicted in Figure 16 is the calculation method of the ISMM (Silva et al., 2012). The ISMM is created to measure the maturity levels of the four main aspects of information security. These four aspects are confidentiality (ICWF), integrity (IIWF), availability (IAWF) and non-repudiation (INWF). An enterprise can use this model to measure the state of their information security policies, assuming they have some information security policies in place and depending on the amount of security policies they have applied regarding their information security management practices.

Percentage	Level
0% ←ISMM ← 20%	Very Low
20% ←ISMM ← 40%	Low
40% ←ISMM ← 60%	Medium
60% ←ISMM ← 80%	High
80% ←ISMM ← 100%	Very High

$$ICWF + IIWF + IAWF + INRWF = 1$$

$$v(a) = \sum_{j=1}^{n} k_j v_j(a)$$

Figure 16 (Case Study) Information Security Maturity Model (Silva et al., 2012)

FOUNDATION

With the use of a literature review, the researchers have identified 26 papers. These papers suggest various information security policies that enterprises should implement to keep their information secure. In some papers, the authors base their view on empirical research and other use their experience and theory.

MATURITY CONSTRUCTION

The ISMM uses five maturity levels. **Level 1: Very Low;** enterprises are not aware about the risks of limited to none information security policy implementations. **Level 2: Low**; enterprises have some awareness about information security and the risks. Some security information is harvested, but not analyzed. **Level 3: Medium**; information security policies are implemented, but there is a bad balance of compliance. Security information is monitored and improvements are planned. **Level 4: High**;

information security policies are implemented and there is a good balance of compliance. There is a constant information security risk and impact analysis, although minor gaps and lapses should be improved. **Level 5: Very High**; there is a full implementation of information security policies and plans, employees are fully aware and compliant. Information security is integrated with applications and considered during design stages.

DOMAIN CONSTRUCTION

Like previously mentioned the model makes use of four domains, these domains are confidentiality, integrity, availability and non-repudiation. These domains are derived for a paper by Shirtz & Elovici (2011). Within these four domains, the authors define 29 information security policies, which are derived from a literature review.

STRENGTHS

One of the stronger elements in the ISMM, is the calculation method which is used to define the maturity level of an enterprise. This calculation method is very objective and uses a solid calculation method as depicted in Figure 16. The other is the assessment instrument that is used to measure maturity in this model is objective, it is only possible to answer yes or no, you have it implemented or not.

INFORMATION SECURITY FOCUS AREA MATURITY MODEL (ISFAM)

Depicted in Figure 17 is the ISFAM (Spruit & Roeling, 2014). The model is designed to support SMEs in designing their information security program. With the use of the ISFAM, SMEs can measure their information security maturity and identify dependencies between various measures in information security. The objective is to structurally improve maturity. When SMEs use this model in the design process of their information security program, it will result in high level guidelines which can be used to improve their current state.

Focus Area: Maturity Level:	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
1. Risk Management				A		B		C			D		
2. Policy Development			A		B						C		
3. Organizing Information Security		A			B					C		D	
4. Human Resource Security				A		B		C		D			
5. Compliance				A		B						C	
Technical													
6. Identity and access management					A		B		C		D		
7. Secure software development					A		B			C		D	
Organizational and Technical													
8. Incident management			A			B			C			D	
9. Business Continuity Management				A		B		C			D		E
10. Change Management				A		B		C		D			
Support													
11. Physical and environmental security						A		B		C			D
12. Asset Management			A				B			C		D	
13. Architecture				A		B			C		D		
	Design					*Implementation*		*Operational Effectiveness*			*Monitoring*		

Figure 17 Information Security Focus Area Maturity Model (Spruit & Roeling, 2014)

FOUNDATION

The foundation of the ISFAM is derived from the ISO27002:2005 standard (ISO, 2005b), the CISSP course (ISC2, 2011), the Standard of Good Practice of the Information Security Forum, the information security framework (ISO-light) and the IBM Framework.

MATURITY CONSTRUCTION

The ISFAM has 12 maturity levels, which are divided in four maturity stages. **1: Level 0 – 4: Design**; the capabilities within the domains are in the design phase, policies are developed and KPIs are defined. **2: Level 5 – 6 Implementation**; roles and responsibilities are defined within the enterprise and standardized processes are developed. **3: Level 7 – 9: Operational Effectiveness**; an enterprise is able to prove that policies and processes are implemented in the way they are designed. **3: Level 10 – 12: Monitoring**; this stage comprehends regularly execution of the first three stages, an enterprise reviews its own policies, procedures and processes and are updated if needed.

DOMAIN CONSTRUCTION

12 of the 13 focus areas are translated from the ISO27002:2005 standard (ISO, 2005b), the focus area Architecture is derived from the CISSP course (ISC2, 2011). Some standards/frameworks described in the chapter Foundation have more domains, but these domains where overlapping with others and have been merged.

STRENGTHS

The maturity construction used in this maturity model is one of the more interesting aspects. Mostly the high amount of levels divided in the four stages is interesting. Since there are many levels, enterprises can go easily a level up, which lowers the barriers of implementation.

3.2 CONCLUSION

Based on the comparison study it can be concluded that there is not a maturity model that follows the principles of Zero Trust. Some of the maturity models contain certain concepts or measures as the Zero Trust principle prescribes. Especially the concept inspect and log all traffic seem to be missing. Other measures regarding the network architecture are also not part of the domains within the seven compared maturity models. Table 7 depicts an overview of the Maturity Model Comparison.

Table 7 Maturity Model Comparison Overview

Maturity Model	Foundation	Maturity	Domains	View
Five Stage to Information Security (5S2IS)	ISO27001:2005, ISO27002:2005 & CMM	Commitment, Systematic, monitored, Improving & Embedded	Based on code of conduct from the ISO27002:2005	High-level overview of domains within IS
Information Security Maturity Model (ISMM)	COBIT, TOGAF, Service Mgmt & Enterpriseal Culture	None, Initial, Basic, Acceptable & Full Compliance	People, Information, Systems and Networks.	Low-level overview of measures within IS
Community Cyber Security Maturity Model (CCSMM)	N/A	Initial, Advanced, Self Awareness, Integrated & Vanguard	Three dimensions: Maturity, Entity and Cybersecurity Capability	High-level overview of cybersecurity and entities
(e-Government) Information Security Maturity Model (ISMM)	ISM3, PRISMA & GISMM	Undefined, Defined, Managed, Controlled & Optimized	Management, Evaluation and Awareness	High-level overview of IS
GAIA Maturity Level Information Security (GAIA-MLIS)	ISO27001:2005, ISO27002:2005 & COBIT	No Insurance, Entry Level Insurance, Regular Insurance, Partially Safe, Fully insured	Hardware, Staff, Software, Facilities & Information	Mid-level overview of information security
(Case Study) Information Security Maturity Model (ISMM)	Literature Study resulted in 26 papers	Very Low, Low, Medium, High, Very High	Confidentiality, Integrity, Availability and Non-Repudiation	Low-level overview of information security
Information Security Focus Area Maturity Model (ISFAM)	ISO27002:2005, CISSP, ISO-light, ISF & IBM	12 levels in four stages: Design, Implementation, Operational Effectiveness & Monitoring	12/13 from ISO27002:2005 & 1/13 from CISSP	High-level overview of Information security

Overall the seven maturity models contain certain aspects that are reused in the construction of the ZeTuMM. The reusable aspects derived from the analysis study are the following:

1. Stepwise Approach for Implementation;
2. Computer-Based Tool to Guide Implementation;
3. Appropriate Distribution of Capabilities;
4. Technical and Enterpriseal Aspects;
5. Cybersecurity Information Sharing;
6. Security Assessments;
7. Calculation Method;
8. Graphical Maturity Representation;

Stepwise Approach for Implementation

Gillies (2011) concluded that cybersecurity is becoming more and more important for SMEs, only the ISO 27001 is only slowly adopted. Evidence shows that this slow adoption rate is mostly because of the complexity and cost of such an implementation. The solution for this problem would be a stepwise approach to implement security measures. With a stepwise approach an enterprise can make smaller steps during the implementation of security frameworks. These smaller steps will also mean that smaller investments are needed for implementation projects.

Computer-Based Tool to Guide Implementation

Gillies (2011) also suggest that a computer-based tool should be used to generate the implementation method in an efficient manner. This computer-based tool should be able to provide progress reports. With the use of progress reports, progress can be monitored and evaluated in a timely manner. This is necessary to control and adjust the implementation projects accordingly.

Appropriate Distribution of Capabilities

Spruit & Roeling (2014) concluded that it is necessary to provide an appropriate wide range of capabilities to make sure the model can be use d as a guideline and roadmap for the implementation of security metrics. The capabilities were defined by using existing maturity models, in some cases new maturity models were created by using the CMM approach. Placement of the capabilities were determined in two ways. Firstly, based on the dependencies of capabilities which were found in literature. Secondly, by using deducible dependencies that arose from expert interviews where a top-down approach for placement was verified.

Technical and Enterpriseal Aspects

Three maturity models mention the differentiation of technical and enterpriseal aspects. In the Information Security Focus Area Maturity Model (ISFAM) a clear distinction is made between Enterpriseal and Technical Focus Areas. Enterpriseal focus areas are mostly categorized by enterpriseal statements and Technical Focus Areas are technically oriented and require a technical implementation (Spruit & Roeling, 2014);

Cybersecurity Information Sharing

The Community Cyber Security Maturity Model (CCSMM) is a maturity model created for communities to improve cybersecurity. The CCSMM has one block with five maturity levels dedicated to cybersecurity information sharing within communities, enterprises and government. To create a clear picture of the current thread landscape communities should be able to share information between each other (White, 2011).

Security Assessments

To be prepared and effectively respond to real threat events, it is important that cybersecurity employees know their role in the response processes and procedures. Besides that, it is just as important to test processes, procedures and technology to test how they respond to various situations. Thus, enterprises should incorporate cybersecurity exercises - where employees practice processes

and procedures and tests where the effectiveness of technology is tested - within an enterprise to measure state of preparedness (White, 2011).

Calculation Method

With the use of a calculation method to calculate maturity, the maturity of an enterprise can be measured. This should be done by giving weight to each cybersecurity control within the model. The (Case Study) Information Security Maturity Model (ISMM) makes use of variable weight distribution for Confidentiality, Integrity, Availability and Non-repudiation. The weight factor for Confidentiality, Integrity, Availability and Non-repudiation can differ for enterprises since one of these aspects can be more important than others (Silva et al., 2012).

Graphical Maturity Representation

When displaying the results of the maturity measurements a graphical representation should be used to present the maturity of enterprises. It should be easy for managers to get a clear picture of the measured maturity. According to Spruit & Roeling (2014) the preference in representation should go to spider charts, as most managers are familiar with those.

4 DESIGN ZETUMM

To determine the capabilities within the focus areas, controls and principles from eight frameworks will be extracted. The extracted controls will be synthesized according to the focus areas which have been derived from the systematic literature review and the existing maturity model analysis. The frameworks which have been selected are:

- CIS Critical Security Controls V6.0 (CIS, 2014)
- Generally Accepted Information Security Principles (GAISP) V3.0 (ISSA, 2003)
- Information Assurance for Small and Medium Sized Enterprises Issue 3.0-2015 (IASME Consortium, 2015)
- ISO/IEC 27002:2013 (ISO, 2013)
- NIST Special Publication 800-14 (NIST, 1996)
- NIST Special Publication 800-27 Rev A (NIST, 2004)
- NIST Special Publication 800-53 (NIST, 2006)
- NIST: Framework for Improving Critical Infrastructure Cybersecurity V1.0 (NIST, 2014)

The previous mentioned frameworks are chosen because they are widely used within the field of IT security. The frameworks are not specific to a sector and generally used. Within the Netherlands, especially the ISO 27001 and 27002 are widely used by companies.

This chapter describes:

1. Design Process ZeTuMM;
2. ZeTuMM Description;
3. Changes to Focus Areas;
4. Tools;

4.1 DESIGN PROCESS ZETUMM

In order to design the focus areas within the ZeTuMM, the scientific approach by (Steenbergen, Bos, Brinkkemper, Weerd, & Bekkers, 2010) will be used. This approach contains guidelines for the development of Focus Area Maturity Models (FAMM). In total this approach consists of four phases, which contain 10 steps. The four phases are:

1. Scoping;
2. Design Model;
3. Develop Instrument;
4. Implement and Exploit.

SCOPING

1. **Identify and scope the function domains:** During this activity, the domain will be scoped by deciding what to include or exclude. Existing (focus area) maturity models will be identified and comparable domains should be used as a base for further development.

DESIGN MODEL

2. **Determine focus areas:** Literature studies, expert interviews and case studies should be used to determine the focus areas. In total around 20 focus areas, should be defined, which should be grouped in smaller focus area groups to improve accessibility.
3. **Determine capabilities:** Every focus area has different capabilities representing grow in maturity levels, depending how these can be developed in an evolutionary way. Determination of these capabilities is based on literature review and expert discussions.
4. **Determine dependencies:** Since the capabilities represents grow in maturity levels, the capabilities have various dependencies based on the preferred order of implementation.
5. **Position capabilities in matrix:** Based on the dependencies and practicality of implementation the capability is positioned in the maturity matrix.

Develop Instrument

6. **Develop assessment instrument:** To use the FAMM as a measure instrument for assessment of the current maturity levels, measures must be defined. This should be done by formulating control questions per capability.
7. **Define improvement actions:** To support movement towards capabilities, improvement actions must be defined. These improvement actions should be described suggestive.

Implement and Exploit

8. **Implement maturity model:** By means of holding expert interviews the model will be validated.
9. **Improve matrix iteratively:** After the expert interviews, a quantitative evaluation should be executed. The model should be adjusted according to the results.
10. **Communicate results:** After completion of the model, the model should be communicated to practitioners as well as the scientific community.

4.2 ZeTuMM Description

The ZeTuMM is designed according to Zero Trust principles and includes controls to take care of corporate-wide cybersecurity best-practices. It offers enterprises a complete solution to become mature and leading in cybersecurity with Zero Trust as focal point. The ZeTuMM consists out of five Focus Area Groups (FAG), these groups host fifteen Focus Areas (FA), which combined prescribe 53 capabilities and offer 428 control questions. Various controls will have elemental dependencies, of which some controls regarding policy will have multiple. Based on the size of an enterprise, enterprise infrastructure and IT management strategies, it can be decided that specific capabilities and controls, up to entire focus areas, are not applicable. This chapter contains the following sections:

Permission

This FAG contains a set of capabilities that together look after the concepts prescribed by Zero Trust as least privilege & access control and ensure secure access specifically for used information systems. Controls within this group make it impossible to move laterally within the network when the network has been breached and contains controls to securely configure access to information systems.

This group contains FAs:

1. Ensure Secure Access (ESA);
2. Information System Security (ISS);
3. Least Privilege & Access Control (LPAC).

Ensure Secure Access (ESA)

Ensure Secure Access (ESA) is achieved by eliminating the trust in an internal network, data will be protected in a similar way as data from the external network. It is achieved by implementing controls from capabilities regarding:

1. Authentication;
2. Conditions and Functional.

Authentication

Authentication is the capability that determines whether the user is genuinely who it claims to be.

Table 8 Authentication capability maturity construction

ESA	Authentication
A	1. Regularly updated identification and authentication policy is used as design foundation. (NIST IA-1) 2. Users are required to authenticate their claimed identities on IT systems. (NIST 3.11.2.1 & NIST Principle 32)
B	1. Users are required to change their passwords periodically. (NIST 3.1.3.3) 2. Password management systems are interactively ensuring quality passwords. (ISO/IEC 9.4.3)
C	1. Access is controlled by a secure log-on procedure when required by the access control policy. (ISO/IEC 9.4.2 & CIS 5.6, CIS 5.7, CIS 11.4, CIS 12.6, CIS 14.5, CIS 16.11, CIS 16.12) 2. Users are required to follow practices in the use of secret authentication information. (ISO/IEC 9.3.1)

D	1. Information system authenticators are managed (NIST IA-5 & NIST 3.11.4.1) 2. Authentication data and tokens are carefully administered and procedures are established. (NIST 3.11.2.6)

Device

With the capability device various configurations of applications and systems is determined.

Table 9 Functional capability maturity construction

ESA	FUNCTIONAL
A	1. Any unnecessary or unauthorized browser or email client plugins or add---on applications are uninstalled or disabled. (CIS 7.2) 2. Loading and executing new software restricted in accordance with regularly updated new software policy. (NIST 3.9.2.1)
B	1. Two separate browser configurations are deployed to each system. (CIS 7.5) 2. The information system checks information inputs for accuracy, completeness, and validity. (NIST SI-10)
C	1. Automated patch management is deployed and patches are applied to all systems. (CIS 4.5) 2. Only fully supported web browsers and email clients are allowed to execute in the enterprise. (CIS 7.1)
D	1. File integrity checking tools to ensure that critical system files have not been altered (CIS 3.5) 2. The information system verifies the correct operation of security functions and reports (NIST SI-6)

INFORMATION SYSTEM SECURITY (ISS)

Information System Security is achieved by properly managing security controls of an Information System. It is achieved by implementing controls from capabilities regarding Compliant, Logical and Physical. It is achieved by implementing controls from capabilities regarding:

Conditions

The capability conditions comprehend a group of controls that set conditions for connection to and from the system that must be met before a connection is authorized.

Table 10 Conditions capability maturity construction

ESA	CONDITIONS
A	1. Secure password attributes are specified and required. (NIST 3.11.3.1) 2. Access is restricted in accordance with the regularly updated access control policy. (ISO/IEC 9.4.1 & NIST PR.PT-3)
B	1. Authentication data is protected as it is entered into the IT system. (NIST 3.11.2.5) 2. The information system provides feedback to a user during an attempted authentication. (NIST IA-6)
C	1. Access Control Lists are implemented that gives permission to use system resources. (NIST 3.12.2.1, CIS 14.4 & CIS 16.9) 2. The information system notifies the user about previous login (attempts). (NIST AC-9)

D	1. All methods of remote access are documented, monitored, and controlled (NIST AC-17, IASME 4.4.6, NIST PR.AC-3 & ISO/IEC 6.2.2) 2. The information system displays an approved, system use notification message before granting system access (NIST AC-8 & NIST 3.9.8)

1. ;
2. Logical;
3. Physical.

Conditions

The capability conditions comprehend a group of controls that set conditions for connection to and from the system that must be met before a connection is authorized.

Table 10 Conditions capability maturity construction

ESA	CONDITIONS
A	3. Secure password attributes are specified and required. (NIST 3.11.3.1) 4. Access is restricted in accordance with the regularly updated access control policy. (ISO/IEC 9.4.1 & NIST PR.PT-3)
B	3. Authentication data is protected as it is entered into the IT system. (NIST 3.11.2.5) 4. The information system provides feedback to a user during an attempted authentication. (NIST IA-6)
C	3. Access Control Lists are implemented that gives permission to use system resources. (NIST 3.12.2.1, CIS 14.4 & CIS 16.9) 4. The information system notifies the user about previous login (attempts). (NIST AC-9)
D	3. All methods of remote access are documented, monitored, and controlled (NIST AC-17, IASME 4.4.6, NIST PR.AC-3 & ISO/IEC 6.2.2) 4. The information system displays an approved, system use notification message before granting system access (NIST AC-8 & NIST 3.9.8)

Governance

The goal of compliant is to ensure that systems comply to policy, laws, regulations and standards.

Table 11 Compliant capability maturity construction

ISS	COMPLIANT
A	1. Regularly updated security assessment and certification and accreditation policy is used as design foundation. (NIST CA-1)
B	1. Directives, laws, enterpriseal culture, guidelines, procedures, and enterpriseal mission are considered. (NIST 3.1.4.4)
C	1. Information systems are regularly reviewed for compliance with policies and standards. (ISO/IEC 18.2.3)
D	1. The information system is accredited for processing before operations and the authorization is updated. (NIST CA-6)

Logical

Logical is a group of controls that defines cybersecurity safeguards the systems takes externally. Controls are mostly on connections to and from the Information System.

Table Logical capability maturity construction

ISS	LOGICAL
A	1. Regularly updated system and information integrity policy is used as implementation foundation. (NIST SI-1) 2. The information system limits the number of concurrent sessions. (NIST AC-10) 3. The information system enforces a limit of consecutive invalid access attempts. (NIST AC-7)
B	1. Use of scripting languages in browsers and email clients is limited. (CIS 7.3) 2. The information system automatically terminates an inactive session. (NIST AC-12) 3. The information system terminates a network connection at the end of a session or inactivity. (NIST SC-10)
C	1. A session lock that remains in effect until the user reestablishes access is initiated. (NIST AC-11) 2. The information system monitors and controls communications at the external boundary and at key internal boundaries. (NIST SC-7) 3. Remote activation of collaborative computing mechanisms is prohibited. (NIST SC-15)
D	1. Host-based authentication grants access based upon the identity of the host originating the request. (NIST 3.12.2.6) 2. A port protection device (PPD) authorizes access to the port itself. (NIST 3.12.2.4) 3. Usage restrictions and implementation guidance for portable and mobile devices are established. (NIST AC-19)

Physical

Controls in the capability physical are constrains that should be configured within the information system.

Table Physical capability maturity construction

ISS	PHYSICAL
A	1. The information system identifies and handles error conditions in an expeditious manner. (NIST SI-11) 2. The information system to provide only essential capabilities and specifically prohibits and/or restricts specific functions. (NIST CM-7)
B	1. Service constraints restrictions, depending on parameters, arise during application use or are pre-established by the resource owner. (NIST 3.12.1.6) 2. The information system isolates security functions from non-security functions. (NIST SC-3)
C	1. Access restrictions associated with changes to the information system are enforced. (NIST CM-5) 2. The information system limits the use of resources by priority. (NIST SC-6)
D	1. To maintain the security of electronic commerce services. (IASME 4.7.3) 2. Specific functions for which users do not have access are restricted. (NIST 3.12.2.2)

LEAST PRIVILEGE & ACCESS CONTROL (LPAC)

Least Privilege & Access Control is achieved by minimizing the amount of resources and applications a user can access. It will ensure that users are only authorized to access resources and applications that they need to perform their work. It is achieved by implementing controls regarding capabilities Accounts, Authorizations and Controls.

1. Account;
2. Control.

Account

Account is the capability that prescribes procedures regarding account management.

Table 12 Account capability maturity construction

LPAC	ACCOUNT
A	1. A process for requesting, establishing, issuing, and closing user accounts is established. (NIST 3.5.2.1) 2. Interviews are conducted employment is terminated and access to the information system is revoked. (NIST PS-4)
B	1. After a set number of failed login attempts the account is locked. (CIS 16.7) 2. Activities of users are supervised and reviewed with respect to the enforcement and usage of information system access controls. (NIST AC-13)
C	1. Allocation of secret authentication information is controlled through a formal management process. (ISO/IEC 9.2.4) 2. User IDs that are inactive on the system for a specific period of time are disabled. (NIST 3.11.1.4)
D	3. Automated tools to inventory all administrative accounts and validate privileges. (CIS 5.2) 4. Access to a particular account is granted only for the duration of a transaction. (NIST 3.12.1.5)

Control

Control is the capability in which manner access to resources within the infrastructure should be controlled.

Table 13 Controls capability maturity construction

LPAC	CONTROL
A	1. Regularly updated access control policy is used as implementation foundation. (NIST AC-1) 2. Administrators are required to access a system with fully logged and non-administrative account. (CIS 5.8)
B	1. Administrators use dedicated machines for all administrative tasks or tasks requiring elevated access. CIS 5.9) 2. Network engineers use dedicated machines for all administrative tasks or tasks requiring elevated access. (CIS 11.6)

C	1.	Wireless device connected to the network match an authorized configuration and security profile. (CIS 15.1)
	2.	Appropriate enterpriseal officials authorize the use of wireless technologies. (NIST AC-18)
D	1.	client certificates are used to validate and authenticate systems prior to connecting to the network. (CIS 1.6)
	2.	Host-based data loss prevention enforces ACLs when data is copied off a server. (CIS 13.9)

INFRASTRUCTURE

Within this FAG controls that are used look after the concept Ensure Secure Access as prescribed Zero Trust. Ensure Secure Access is achieved by configuring handling rules for static data and data in traffic within, to and from the infrastructure, separating the network in small chunks and manage the network from the inside-out. Controls within the group focus on the network and data security combined with controls to manage digital assets.

This group contains FAs:

1. IT Life-Cycle (ITLC);
2. Data Life-Cycle (DLC);
3. Information System Life-Cycle (ISLC);
4. Network Segmentation (NS).

IT LIFE-CYCLE (ITLC)

Shadow IT is a term used to define unsupported software and hardware that is used within the network. It will ensure that only devices are having authorized to access resources and applications that they need to perform their work. It is achieved by implementing controls regarding capabilities:

1. Asset;
2. Configuration;
3. Maintenance;
4. Management.

Asset

Asset is the capability that prescribes in which manner corporate assets should be managed.

Table 14 Asset capability maturity construction

ITLC	ASSET
A	1. An asset inventory of all systems and network devices is maintained. (CIS 1.4) 2. Software inventory tools are deployed that cover all of the operating system types in use. (CIS 2.3)
B	1. A list of authorized software and version that is required in the enterprise is devised. (CIS 2.1) 2. Security for different risks of working outside the enterprise's premises is applied to off-site assets. (ISO/IEC 11.2.6)
C	1. Assets entering and exiting the facility are controlled and appropriate records are maintained. (NIST PE-16) 2. Procedures for the management of removable media are implemented in accordance with a classification scheme. (ISO/IEC 8.3.1)
D	1. Automated asset inventory discovery tools are deployed to build inventory. (CIS 1.1) 2. Application whitelisting is deployed and configured to only allow whitelisted software. (CIS 2.2)

Configuration

The capability configuration hosts controls regarding certain configurations that should be applied to assets.

Table 15 Configuration capability maturity construction

ITLC	CONFIGURATION
A	1. Screen locks are configured on systems to limit access to unattended workstations. (CIS 16.5) 2. Access to system files and source code is controlled. (IASME 4.8.1)
B	1. A baseline configuration is developed, documented, and maintained. (NIST CM-2) 2. Configuration management tools that will automatically enforce and redeploy configuration settings is implemented. (CIS 3.7)
C	1. information system maintenance tools are maintained and approved, controlled, and monitored when used on a regular basis. (NIST MA-3) 2. The information system can detect and protect against unauthorized changes. (NIST SI-7)
D	1. All alterations to configuration files are logged and automatically reported to IM. (CIS 11.3) 2. Master images are stored on securely configured servers. (CIS 3.3)

Maintenance

The capability maintenance is a group of controls that prescribes in which manner maintenance should be performed on the infrastructure.

Table 16 Maintenance capability maturity construction

ITLC	MAINTENANCE
A	1. Regularly updated maintenance policy is used as implementation foundation. (NIST MA-1) 2. Maintenance support and spare parts for assets are obtained. (NIST MA-6)
B	1. A list of authorized personnel to perform maintenance is maintained. (NIST MA-5) 2. Procedures are developed to ensure that only authorized personnel perform maintenance. (NIST 3.9.7)
C	1. The latest stable versions of security-related updates are installed on all network devices. (CIS 11.5) 2. Routine preventative and regular maintenance on the components is scheduled, performed, and documented. (NIST MA-2)
D	1. all remote administration is performed over secure channels. (CIS 3.4) 2. Security testing of entire system as well as particular parts is performed. (NIST 3.4.4.2)

Management

The capability management makes sure all IT resources of enterprises are managed according to specific predefined standards.

Table 17 Management capability maturity construction

ITLC	MANAGEMENT
A	1. Regularly updated configuration management policy is implemented and used as a foundation 2. Appropriate controls are established to balance access to information assets and supporting Information Technology resources against the risk.
B	1. All default passwords are changed before deploying any new devices in a networked environment 2. Changes to the information system are documented and controlled
C	1. Changes to the system do not unintentionally or unknowingly diminish security 2. All devices remotely logging into the internal network are managed and controlled
D	1. Changes to the information system are monitored and security impact analyses are conducted to determine the effects of the changes. 2. Devices have corporate-level protection, detection and recovery processes in place

DATA LIFE-CYCLE (DLC)

Data life-cycle an approach that locates, protects and indexes data that are generated by users. It is achieved by implementing controls regarding capabilities Encryption, Identification, Prevention, Protection and Technique.

1. Encryption;
2. Identification;
3. Prevention;
4. Protection.

Encryption

The capability encryption provides security controls to make sure all data – at rest or in transfer – within the enterprise are encrypted.

Table 18 Encryption capability maturity construction

DLC	ENCRYPTION
A	1. Is all wireless traffic leveraged with at least Advanced Encryption Standard (AES) encryption used with at least Wi---Fi Protected Access 2 (WPA2) protected?
B	1. is Authentication data transmitted over public or shared data networks protected?
C	1. Are approved hard drive encryption software deployed to mobile devices and systems that hold sensitive data?
D	1. Is information passing over public networks protected from fraudulent activity?

Identification

The capability identification makes sure all valuable or sensitive data within the enterprise is identified and cataloged.

Table 19 Identification capability maturity construction

DLC	IDENTIFICATION
A	1. Is an assessment of data performed that identifies sensitive information? 2. Is Information classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification?
B	1. Are appropriate procedures information labelling developed and implemented? 2. Are information assets routinely cataloged and valued, and levels of sensitivity and criticality are assigned"?.
C	1. Do automated tools conduct periodic scans server machines for sensitive data? 2. Are the enterpriseal communication and data flows are mapped?
D	1. Can the Information System determent who did what? 2. Are marking and logging to provide physical and environmental protection and accountability?

Prevention

The capability prevention guarantees that interception of data by any means is prevented.

Table 20 Prevention capability maturity construction

DLC	PREVENTION
A	1. A media protection policy is used as design foundation and regularly updated and controls are implemented. 2. All items containing storage media are verified and data disposal is ensured.
B	1. An automated tool is deployed on network perimeters which monitors for sensitive information. 2. The information system prevents unauthorized and unintended information transfer.
C	1. Security parameters are associated by the information system 2. Rules for the acceptable use of information and of assets are identified, documented and implemented.
D	1. Do network---based DLP solutions monitor and control the flow of data within the network? 2. External labels are affixed to removable information storage media.

Protection

The capability protection makes sure that all data within the enterprise is protected in accordance with regulations and priorities.

Table 21 Protection capability maturity construction

DLC	PROTECTION
A	1. Records are protected in accordance with legislatory, regulatory, contractual and business requirements. 2. Agreements address secure transfer of business information between the enterprise and external parties. 3. Appropriate protection of information assets is achieve and maintained.
B	1. Output from the information system is handled and retained in accordance to policy and operational requirements. 2. Risk mitigating measures to prevent interception of data. 3. Media containing information is protected against unauthorized access, misuse and corruption during transportation.
C	1. Information assurance is managed within the enterprise and in relations with partners 2. Long-term requirements regarding the use of data are considered when moving or archiving data 3. Protection processes are continuously improved
D	1. Test for the presence of unprotected system information and artifacts. 2. Information involved in application service transactions is protected. 3. Only authorized users have access to information in printed form.

INFORMATION SYSTEM LIFE-CYCLE (ISLC)

Information System life-cycle an approach that contains controls to manage the information system's life-cycle. It is achieved by implementing controls regarding capabilities Acquisition, Development and Management.

1. Acquisition;
2. Development;
3. Management.

Acquisition

The capability acquisition prescribes specific controls and procedures to buy or obtain information system assets.

Table 22 Acquisition capability maturity construction

ISLC	ACQUISITION
A	1. During the first part of the acquisition phase, security requirements are developed at the same time as the requirements of the system. (NIST 3.4.3.1) 2. A regularly updated policy system and services acquisition is used as design foundation and controls are implemented. (NIST SA-1)
B	1. All equipment acquisitions are automatically as new updated in the inventory system. (CIS 1.3) 2. Trade-offs among security, cost, simplicity, efficiency, and ease of implementation are considered when acquiring security products. (NIST 3.14.2)
C	1. For acquired application software is checked whether the version that is used, is still supported by the vendor (CIS 18.1) 2. Security requirements and/or security specifications in information system acquisitions include contracts based on an assessment of risk. (NIST SA-4)
D	1. Security is considered in acquisition and through-life management of assets 2. (IASME 4.4.1) Acceptance testing programs and related criteria are established for new information systems, upgrades and new versions. (ISO/IEC 14.2.9)

Development

The capability development prescribes specific controls and procedures to start the development of new information systems

Table 23 Development capability maturity construction

ISLC	DEVELOPMENT
A	1. During system development security activities include developing the system's security features and monitoring the development process and security problems. (NIST 3.4.3.3) 2. Information security related requirements are included in requirements for new information systems or enhancements to existing information systems. (ISO/IEC 14.1.1)
B	1. Developers create and configuration management plans that controls changes, tracks security flaws, and provide implementation documentation. (NIST SA-10) 2. The information system is designed and implemented using security engineering principles. (NIST SA-8)

C	1. Operational ease of use is a requirement when developing system (NIST Principle 15) 2. Implement layered security (Ensure no single point of vulnerability) (NIST Principle 16)
D	1. Secure development environments for system development and integration efforts are established and appropriately protected. (ISO/IEC 14.2.6) 2. The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. (NIST SA-11)

Management

The capability management makes sure all information systems of enterprises are managed according to specific predefined standards.

Table 24 Management capability maturity construction

ISLC	MANAGEMENT
A	1. A regularly updated system policy includes system security rules for operating or developing, is used as design foundation and controls are implemented. (NIST 3.2.2.1) 2. Determine security features, assurances, and operational practices to yield significant security information and voluminous requirements. (NIST 3.4.3.2)
B	1. Where possible security is based on open standards for portability and interoperability (NIST Principle 12) 2. The information system is managed using system development life cycle methodology that includes information security considerations. (NIST SA-3)
C	1. Security is designed to allow for regular adoption of new technology, including a secure and logical technology upgrade process (NIST Principle 14) 2. Policies vary because each system needs defined security objectives based on the system's operational requirements, environment, and the manager's acceptance of risk. (NIST 3.1.3.3)
D	1. Custom products to achieve adequate security are considered (NIST Principle 10) 2. Tailored system security measures are implemented to meet security goals (NIST Principle 8)

NETWORK SEGMENTATION (NS)

MCAP or Network segmentation is a concept where the network is divided in various smaller dedicated networks. It is achieved by implementing controls regarding capabilities:

1. Connections;
2. Filtering;
3. Segmentation;
4. Segregation;
5. Unprivileged.

Connections

The capability connections offers controls that should be implemented to manage the connections to, from and in-between information systems.

Table 25 Connections capability maturity construction

NS	CONNECTIONS
A	1. Network based URL filters that limit a system's ability to connect to unapproved websites is maintained and enforced. (CIS 7.6) 2. Communications with known malicious IP addresses is denied or access is only allowed to trusted sites (whitelists). (CIS 12.1)
B	1. Domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains is enabled. (CIS 8.6) 2. The Sender Policy Framework is implemented by deploying SPF records in DNS and enabling receiver-side verification in mail servers (CIS 7.7)
C	1. Access to known file transfer and email exfiltration websites is blocked. (CIS 13.8) 2. All connections and interconnections outside accreditation boundary from the information system to other information systems are authorized and approved by officials. (NIST CA-3)
D	3. Back-channel connections to the Internet that bypass the DMZ are periodically scanned. (CIS 12.8) 4. Host-based firewalls or port filtering tools are implemented with a default deny rule on end systems. (CIS 9.2)

Filtering

The capability filtering specifies controls regarding the filtering of connections to, from and in-between information systems.

Table 26 Filtering capability maturity construction

NS	FILTERING
A	1. Secure gateways block or filter access between two networks. (NIST 3.12.2.5) 2. Prevent data exfiltration by configuring the built-in firewall session tracking mechanisms and alert suspicious TCP sessions (CIS 12.10)
B	1. All email attachments are scanned and blocked if they contain malicious code and specific file types. (CIS 7.8)

	2. Network perimeters are designed and implemented so that all outgoing network traffic passes through an application layer filtering proxy server. (CIS 12.5)
C	1. All traffic leaving is monitored and any unauthorized use of encryption is detected (CIS 13.7) 2. Application firewalls are placed in front of critical servers to verify and validate traffic going to the server. (CIS 9.6)
D	1. Web applications are protected by deployed web application firewalls (WAFs) that inspect all traffic. (CIS 18.2) 2. Network-based IDS sensors deployed to scans and blocks unusual attack mechanisms are and detect compromises. (CIS 12.3)

Segmentation

The capability segmentations lays down controls in which manner data and applications should be segmented within the enterprise's network.

Table 27 Segmentation capability maturity construction

NS	SEGMENTATION
A	1. Privacy and protection of personally identifiable information is ensured as required in relevant legislation and regulation. 2. (ISO/IEC 18.1.4) Security mechanisms, service levels and management requirements services are identified and included in services agreements. (ISO/IEC 13.1.2)
B	1. Networks are managed and controlled to protect information in systems and applications. (ISO/IEC 13.1.1) 2. Separate virtual local area networks for BYOD systems or other untrusted devices is created. (CIS 15.9)
C	1. Network switches enable Private Virtual Local Area Networks for segmented workstation networks. (CIS 14.3) 2. The network infrastructure is managed across network connections that are separated from the business use of networks. (CIS 11.7)
D	1. Network operations and expected data flow baselines for users and systems are established and managed. (NIST DE.AE-1) 2. Based on the label or classification level the network is segmented. (CIS 14.1)

Segregation

The capability segmentations lays down controls in which manner data and applications should be segregated within the enterprise's network.

Table 28 Segregation capability maturity construction

NS	SEGREGATION
A	1. IT system are designed and operated limit damage and to be resilient in response (NIST Principle 17) 2. If a server is not required to be visible from an untrusted network, it is moved to an internal VLAN. (CIS 9.4)

B	1.	Provide that the system is, and continues to be resilient in the face of expected threats is assurance (NIST Principle 18)
	2.	Groups of information services, users and information systems are segregated on networks. (ISO/IEC 13.1.3)
C	1.	VMs are used to isolate and run applications that are required for business operations but are too risky on networked systems (CIS 2.4)
	2.	By incorporating network segregation where appropriate, the network integrity is protected, (NIST PR.AC-5)
D	1.	Separate environments for production and nonproduction systems are maintained. (CIS 18.6)
	2.	Communications and control networks are protected (NIST PR.PT-4)

Unprivileged

The capability unprivileged offers rule sets to design a separated network that can be accessed without login credentials.

Table 29 Unprivileged capability maturity construction

NS	UNPRIVILEGED	
A	1.	Public access systems are isolated from mission critical resources. (NIST Principle 20)
	2.	Network level authentication is deployed via 802.1x to limit and control devices. (CIS 1.5)
B	1.	External systems are assumed to be insecure. (NIST Principle 6)
	2.	Network vulnerability scanning tools are configured to detect wireless access points connected to the wired network. (CIS 15.2)
C	1.	Specific user actions that can be performed without identification or authentication are identified. (NIST AC-14)
	2.	Wireless intrusion detection systems are used to identify rogue wireless devices and detect attack attempts. (CIS 15.3)
D	1.	The potential impact on the shared global infrastructure is considered when network security measures are established. (GAISP 3.12)
	2.	Wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS). (CIS 15.6)

PROCESSES

Process is a FAG constructed from controls that takes in account relevant cybersecurity aspects of process management. Since Zero Trust itself doesn't specifically prescribe rigor process management concepts or measures, this group is created and constructed with the Zero Trust principles in mind.

This group contains FAs:

1. Contingency Management (CM);
2. Incident Management (IM);
3. Organizational Management (OM);
4. Risk Management (RM)

CONTINGENCY MANAGEMENT (CM)

Contingency management is combined out of capabilities that will manage unexpected events by providing controls that provide operational continuity. It is achieved by implementing controls regarding capabilities:

1. Assurance;
2. Capacity;
3. Environmental;
4. Planning.

Assurance

The capability assurance provides controls that declares the availability of information systems during 'unexpected' events.

Table 30 Assurance capability maturity construction

CM	ASSURANCE
A	1. The contingency plan is implemented, appropriate preparations are made and procedures are documented. (NIST 3.6.4.4) 2. Requirements for information security and the continuity of information security management during a crisis or disaster is determined. (ISO/IEC 17.1.1)
B	1. A likely range of problems which include small and large contingencies is identified. (NIST 3.6.3.1) 2. Responsibility for keeping the contingency plan current are specifically assigned. (NIST 3.6.5.1)
C	1. Contingency measures and effective recovery processes are in place to mitigate impact of possible contingencies. (IASME 4.12.4) 2. Primary and alternate telecommunications services are identified and necessary agreements for resumption during contingencies are made. (NIST CP-8)
D	1. There are joined up enterprise and business unit level contingency plans to counteract and recover from contingencies. (IASME 4.13.3) 2. Alternate processing sites are identified and necessary agreements for resumption are made. (NIST CP-7)

Capacity

The capability capacity specifies controls to guarantees that information systems have sufficient computing powers.

Table 31 Capacity capability maturity construction

CM	CAPACITY
A	1. Time frames in which each resource is used is identified in combination with effects on the business by unavailability. (NIST 3.6.2.4) 2. Adequate capacity is maintained to ensure availability. (NIST PR.DS-4)
B	1. Identification of resources is a managers' area of responsibility. (NIST 3.6.2.2) 2. Commonly used resources list is created that contains resources which are used most. (NIST 3.6.2.3)
C	1. Usage of resources is monitored, tuned and projections made of future capacity requirements. (ISO/IEC 12.1.3) 2. Based on their classification, criticality, and business value resources are prioritized. (NIST ID.AM-5)
D	1. The information system and the information processed, stored, or transmitted is categorized in accordance with FIPS 199. (NIST RA-2) 2. As part of capital planning and investment control resources to protect the information system are determining, documented, and allocated. (NIST SA-2)

Environmental

The capability environmental provides controls that declares the availability of information systems during 'unexpected' events in the surroundings of the information systems.

Table 32 Environmental capability maturity construction

CM	ENVIRONMENTAL
A	1. The information system is protected from water damage. (NIST PE-15) 2. A regularly updated physical and environmental protection policy is used as design foundation and controls are implemented. (NIST PE-1)
B	1. Systems and operators are operated in decently-controlled operating environment. (NIST 3.10.3) 2. Fire suppression and detection devices/systems are employed and maintained. (NIST PE-13)
C	1. Equipment is sited and protected to reduce the risks from environmental threats and hazards. (ISO/IEC 11.2.1) 2. Power equipment and power cabling for information system is protected. (NIST PE-9)
D	1. Physical protection against natural disasters, malicious attack or accidents are designed and applied. (ISO/IEC 11.1.4) 2. Awareness about severe and full destructive contingencies is assured. (NIST 3.10.4)

Planning

The capability planning offers various procedural measures to provides roadmaps and guidelines during 'unexpected' events.

Table 33 Planning capability maturity construction

CM	PLANNING
A	1. Critical business processes are protected from the effects of major contingencies. (IASME 4.13.2) 2. A regularly updated contingency planning policy is used as design foundation and controls are implemented. (NIST CP-1)
B	1. Fire safety controls of buildings that house systems are evaluated. (NIST 3.10.2) 2. The relationship between recovery and resumption to return to normal operations is determine. (NIST 3.6.4.3)
C	1. Analysis of needed resources is conducted by those who understand the functions the interdependencies among resources. (NIST 3.6.2.1) 2. For specific locations capabilities of shutting off power are provided for any information technology component that could malfunction. (NIST PE-10)
D	1. The contingency scenarios address all commonly used resource listed above. (NIST 3.6.3.2) 2. All aspects of computer support and operations are documented to ensure continuity and consistency. (NIST 3.9.6)

INCIDENT MANAGEMENT (IM)

Incident management helps to prevent security incidents by detecting, prioritizing and addressing vulnerabilities in the IT infrastructure of an enterprises. It is achieved by implementing controls regarding:

1. Management;
2. Report;
3. Resolve;
4. Response.

Management

The capability management makes sure incidents of enterprises are managed by the incident handling team according to specific predefined standards.

Table 34 Management capability maturity construction

IM	MANAGEMENT
A	1. Technical staff that handles incidents have specific knowledge and prepositioned technical capabilities. (NIST 3.7.2.4) 2. There are written incident response procedures including definitions of personnel roles for incident handling (CIS 19.1)
B	1. Responsibilities and procedures for management are established. (ISO/IEC 16.1.1) 2. Incident information is promptly reported to appropriate authorities. (NIST IR-6)
C	1. Recovery practices are effectively communicated to different types of users. (NIST 3.7.2.5) 2. Appropriate parties are informed about event detection. (NIST DE.DP-4)
D	1. Job titles and duties for handling computer and network incidents assigned to specific individuals. (CIS 19.2) 2. Contacts with other groups who could assist in incident handling and in containment and recovery efforts are pre-established. (NIST 3.7.2.6)

Report

The capability report lays down specific guidelines in which manners incidents should be reported to the incident handling team.

Table 35 Report capability maturity construction

IM	REPORT
A	1. Enterprise-wide standards are devised for personnel to report anomalous events to the incident handling team. (CIS 19.4) 2. An incident response support resource that offers advice and assistance for the handling and reporting of security incidents is provided. (NIST IR-7)
B	1. Information on third-party contact information is assembled and maintained and used to report a security incident. (CIS 19.5) 2. Information system flaws are Identified, reported, and corrected. (NIST SI-2)
C	1. When using information systems and services employees and contractors are required to note and report information security weaknesses. (ISO/IEC 16.1.3)

	2. Procedures for the identification, collection, acquisition and preservation of information are defined and applied. (ISO/IEC 16.1.7)
D	1. Information security events and weaknesses are identified and reported within agreed timeframes (IASME 4.12.1) 2. Thresholds to create incident alert are established. (NIST DE.AE-5)

Resolve

The capability resolve prescribes in which manner the incident handling team should be able to resolve reported incidents.

Table 36 Resolve capability maturity construction

IM	RESOLVE
A	1. The capability to respond to and resolve information security incidents is provided. (GAISP 3.7) 2. During or after an event the recovery plan is executed. (NIST RC.RP-1)
B	1. Audit trails are used to support after the fact investigations. (NIST 3.13.2) 2. Capabilities to to recover from the effects of malware are in place. (IASME 4.9.2)
C	1. Likelihood of similar incidents is reduced by evaluations of information security incidents. (ISO/IEC 16.1.6) 2. During a failure of an information system and subsequent recovery confidentiality of information is retained. (IASME 4.13.5)
D	1. The security incident handling department assist other enterprises and helps to protect the whole community. (NIST 3.7.2.1) 2. Forensics is performed. (NIST RS.AN-3)

Response

The capability response lays defines controls in which manner the incident handling team should respond to reported incidents.

Table 37 Response capability maturity construction

IM	RESPONSE
A	1. Information security events are assessed and decided if they are classified as security incidents. (ISO/IEC 16.1.4) 2. A regularly updated incident response policy is used as design foundation and controls are implemented. (NIST IR-1)
B	1. The impact and consequences of the incidents are understood. (NIST RS.AN-2) 2. Information system security alerts/advisories are received on a regular basis and issues alerts/advisories are reported to appropriate personnel. (NIST SI-5)
C	1. Categorization of incidents is consistent with response plans. (NIST RS.AN-4) 2. Mitigating incidents is the first response. (NIST RS.MI-2)
D	1. To understand attack targets and methods events are analyzed. (NIST DE.AE-2) 2. During containment of incidents an assessment is included whether the incident is part of a targeted attack. (NIST 3.7.1.2)

ORGANIZATIONAL MANAGEMENT (OM)

The goal of this focus area is to provide an enterprise various controls to manage and protect the enterprise from cyber threats. It is achieved by implementing controls regarding:

1. Physical;
2. Procedure;
3. Roadmap.

Physical

The capability physical lays down specific physical controls to protect the enterprise against physical infiltrations of buildings.

Table 38 Physical capability maturity construction

OM	PHYSICAL
A	1. Temperature and humidity within facilities containing information systems is controlled and maintained. (NIST PE-14) 2. A regularly updated operating environment for assets policy is used as design foundation and controls are implemented. (NIST PR.IP-5)
B	1. Physical access controls restrict the entry and exit of personnel. (NIST 3.10.1) 2. A current lists of authorized personnel is developed and updated and appropriate authorization credentials are issued. (NIST PE-2)
C	1. Security perimeters are defined and used to protect the information systems and information. (ISO/IEC 11.1.1) 2. Physical security controls for offices, rooms and facilities is designed and applied. (ISO/IEC 11.1.3)
D	1. To detect potential cybersecurity events, the physical environment is monitored (NIST DE.CM-2) 2. Telecommunications cabling carrying data and supporting information services are protected from interception, interference or damage. (ISO/IEC 11.2.3)

Procedure

The capability procedure lays down procedures the enterprises should implement to guarantee solid cybersecurity governance.

Table 39 Procedure capability maturity construction

OM	PROCEDURE
A	1. Information security is addressed in project management, regardless type of project. (ISO/IEC 6.1.5) 2. Appropriate and agreed levels of security and service delivery with third parties are implement and maintain (IASME 4.7.2)
B	1. Procedures for working in secure areas are designed and applied. (ISO/IEC 11.1.5) 2. Management direction and support for information security is provided in accordance with business requirements (IASME 4.3.1)
C	1. Management makes decisions based on a technical analysis. (NIST 3.1.3.2)

	2. The approach to managing information security and its implementation is reviewed independently at intervals or after changes. (ISO/IEC 18.2.1)
D	1. A formal sanctions process when failing to comply with information security policies and procedures is employed. (NIST PS-8) 2. Privacy impact assessments are conducted on the information system. (NIST PL-5)

Roadmap

The capability roadmap describes which roadmaps should be created to guarantee solid cybersecurity governance.

Table 40 Roadmap capability maturity construction

OM	ROADMAP
A	1. A regularly updated plan of action and milestones is used as design foundation and controls are implemented. (NIST CA-5) 2. A security plan for the information system is developed and implemented to provides an overview security controls in place or planned. (NIST PL-2) 3. When developing and describing security requirements common language is used. (NIST Principle 13)
B	1. Position statement, applicability, roles and responsibilities, compliance, and point of contact are communicated. (NIST 3.1.2.3) 2. Established programs are knowledgeable and take advantage of external sources of information. (NIST 3.2.1.7) 3. The program management function is stable and recognized within the enterprise as a focal point for computer security. (NIST 3.2.1.1)
C	1. Priorities for enterpriseal mission, objectives, and activities are established and communicated (NIST ID.BE-3) 2. Operating procedures are documented and made available to all users who need them. (ISO/IEC 12.1.1) 3. Decisions taken by management to protect a system should be explicitly stated. (NIST 3.1.3.1)
D	1. The security plan for the information system is reviewed and revised to address system/enterpriseal aspects (NIST PL-3) 2. An effective program establishes relationships with overlapping groups in order to integrate cybersecurity into daily management. (NIST 3.2.1.6) 3. Security measures to address multiple overlapping information domains are formulated. (NIST Principle 31)

RISK MANAGEMENT (RM)

To identify, analyze and control risk to mitigate potential damages of potentially unfortunate expected events. It is achieved by implementing controls regarding capabilities:

1. Analyze;
2. Back-up;
3. Control;
4. Identify.

Analyze

The capability analyze describes in which manner risks – that enterprises face – should be analyzed.

Table 41 Analyze capability maturity construction

RM	ANALYZE
A	1. In assessing risk, the first step is identifying the considered system (part), analytical method and level of detail and formality. (NIST 3.3.1.1) 2. Assessments risk and magnitude of harm that could result from the unauthorized access are conducted. (NIST RA-3)
B	1. Different components of risk are examined including data about the threatened area which is synthesizing and analyzing to information. (NIST 3.3.1.2) 2. Information risk is considered in business context. (IASME 4.2.2)
C	1. The risk tolerance is determined and expressed (NIST ID.RM-2) 2. To determine risk threats, vulnerabilities, likelihoods, and impacts analysis are used. (NIST ID.RA-5)
D	1. Risk assessments are used to accept the risk or selection of cost-effective controls. (NIST 3.3.1.3) 2. Potential trade-offs between reducing risk and increased costs are identified and decreased. NIST Principle 7)

Back-up

The capability back-up specifies in which manner an enterprise should manage their back-up procedures to guarantee availability of information.

Table 42 Back-up capability maturity construction

RM	BACK-UP
A	1. A regularly updated back-up policies is used as design foundation and controls are implemented. (CIS 10.1) 2. Backup copies of information, software and system images are taken and tested regularly in accordance with policy. (ISO/IEC 12.3.1)
B	1. On a regular basis test data on back-up media is properly tested by performing a data restoration process. (CIS 10.2) 2. The integrity and availability of information and information systems is maintained by backup and restore capabilities (IASME 4.11.1)
C	1. Back-ups are properly protected via physical security and encryption when they are stored. (CIS 10.3)

	2. Back-ups of user- and system-level information are back-upped and are stored at an appropriately secured location. (NIST CP-9)
D	1. Key systems have at least one back-up destination that is not continuously addressable through operating system calls. (CIS 10.4) 2. An alternate storage site is identified and initiated agreements are made. (NIST CP-6)

Control

The capability control offers prescribes measures on how risk and risk mitigations should be managed.

Table 43 Control capability maturity construction

RM	CONTROL
A	1. Selected safeguards are effectively implemented and are periodically reanalyzed of risks, assets and improved. (NIST 3.3.2.3) 2. A regularly updated risk assessment policy is used as design foundation and controls are implemented. (NIST RA-1)
B	1. Processes that control cybersecurity risks are governance and risk management. (NIST ID.GV-4) 2. All enterprise stakeholders established, manage, and agree risk management processes. (NIST ID.RM-1)
C	1. Determination of risk tolerance is informed via critical infrastructure and sector specific risk analysis. (NIST ID.RM-3) 2. Appropriate risk management is demonstrated to partners and suppliers. (IASME 4.2.5)
D	1. Risks to the internal and external physical environment are consider and compensate where necessary. (GAISP 3.5) 2. Information assurance to the business is provided by a descent understanding of the information risk. (IASME 4.2.1)

Identify

The capability analyze describes in which manner risks – that enterprises face – should be identified.

Table 44 Identify capability maturity construction

RM	IDENTIFY
A	1. To keep abreast of emerging threats and countermeasures (IASME 4.1.2) 2. Potential business impacts and likelihoods are identified. (NIST ID.RA-4)
B	1. To determine the business risk appetite (IASME 4.2.3) 2. Risk responses are identified and prioritized. (NIST ID.RA-6)
C	1. Internal and external threats are identified and documented. (NIST ID.RA-3) 2. A risk designation is assigns to all positions and screening criteria for individuals filling those positions established and updated. (NIST PS-2)
D	1. Identification of appropriate controls is primary a function of computer security risk management. (NIST 3.3.2.1) 2. The analysis and management of risk are modified when changes to the systems, devices or information occur. (NIST 3.10.7)

INTELLIGENCE

The Intelligence FAG safeguards Inspect & Log Traffic as prescribed by Zero Trust. The FAs advanced threat protection and inspect & log traffic provide controls to monitor the network in real-time. When fully implemented it detects abnormal user and network behavior. As a result, breaches are detected in a timely manner and thus opportunities to effectively apply countermeasures for breach mitigation and/or stopping breaches will arise.

This group contains two FAs:

1. Advanced Threat Protection (ATP);
2. Inspect & Log Traffic (ILT).

ADVANCED THREAT PROTECTION (ATP)

Advanced threat protection can detect known as well as unknown threats exploits and malicious executables. It is achieved by implementing controls regarding capabilities:

1. Detection;
2. Management;
3. Prevention;
4. Sharing.

Detection

The capability detection specifies controls that should be implemented to detect intrusion and extrusion attempts by attackers.

Table 45 Detection capability maturity construction

ATP	DETECTION
A	1. Network-based anti-malware tools are used to identify executables in all network traffic before it arrives at the endpoint. (CIS 8.5) 2. Unauthorized mobile code is detected (NIST DE.CM-5)
B	1. Automated tools are employed to continuously monitor workstations, servers, and mobile devices and detected events are reported. (CIS 8.1) 2. Automated port scans are performed on a regular basis against all key servers and compared to known baselines and changes are reported. (CIS 9.3)
C	1. Vulnerability scanning is performed in authenticated mode via dedicated accounts and tied to machines and IP addresses. (CIS 4.3) 2. Anti-malware with centralized infrastructure that and pushes updates to systems is employed. (CIS 8.2)
D	1. Automated vulnerability scanning tools compile information on reputations to system administrators with risk scores and comparison. (CIS 4.1) 2. Unauthorized intrusion and extrusion is detect. (IASME 4.9.3)

Management

The capability management makes sure advanced threats are managed according to specific predefined systems and procedures.

Table 46 Management capability maturity construction

ATP	MANAGEMENT
A	1. Vulnerability and penetration testing tools are used and results are used for focused penetration testing efforts. (CIS 20.6) 2. A vulnerability management plan is developed and implemented. (NIST PR.IP-12)
B	1. Detection processes are tested. (NIST DE.DP-3) 2. Detection activities comply with all applicable requirements. (NIST DE.DP-2)
C	1. A process for ranking based on risk-rate of vulnerabilities is established to apply patches for the riskiest vulnerabilities first. (CIS 4.8) 2. The results from back-to-back vulnerability scans are verified on addressed risks and are periodically reviewed on effectiveness. (CIS 4.7)
D	1. Detection processes are continuously improved. (NIST DE.DP-5) 2. Information about technical vulnerabilities of information systems being used are obtained in a timely fashion to address the associated risk. (ISO/IEC 12.6.1)

Prevention

The capability prevention lays down specific controls on how intrusion and extrusion of sensitive data can be prevented.

Table 47 Prevention capability maturity construction

ATP	PREVENTION
A	1. The information system implements spam and spyware protection. (NIST SI-8) 2. Anti-exploitation features as DEP, ASLR,EMET and virtualization/containerization are enabled. (CIS 8.4)
B	1. The information system protects against the effects of denial of pre-established service attacks. (NIST SC-5) 2. Detection, prevention and recovery controls to protect against malware are implemented. (ISO/IEC 12.2.1)
C	1. Clear goals of the penetration test are planned with multi-vector attacks in mind. (CIS 20.5) 2. Regular external and internal penetration tests are conducted to identify vulnerabilities and attack vectors. (CIS 20.1)
D	1. Network-based IPS devices are deployed to complement IDS and blocks known bad signatures and behavior of potential attacks. (CIS 12.4) 2. Protections are in place against all likely classes of "attacks" (NIST Principle 11)

Sharing

The capability sharing specifies how information should be shared with the public about infiltration and exfiltration attempts and after breaches.

Table 48 Sharing capability maturity construction

ATP	SHARING
A	1. Public relations are managed. (NIST RC.CO-1) 2. Reputation after an event is repaired. (NIST RC.CO-2)
B	1. Threat and vulnerability information is received from information sharing forums and sources. (NIST ID.RA-2) 2. Subscriptions to vulnerability intelligence services are order and used to update the enterprise's vulnerability scanning activities. (CIS 4.4)
C	1. Appropriate contacts with interest groups and specialized security forums and professional associations are maintained. (ISO/IEC 6.1.4) 2. Effectiveness of protection technologies is shared with appropriate parties. (NIST PR.IP-8)
D	1. Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness. (NIST RS.CO-5) 2. Appropriate contacts with relevant authorities are maintained. (ISO/IEC 6.1.3)

INSPECT & LOG TRAFFIC (ILT)

By inspecting and logging all traffic in real-time, abnormal user behavior and network traffic can be detected. It is achieved by implementing controls regarding capabilities:

1. Audit;
2. Log;
3. Manage;
4. Monitor.

Audit

The capability audit specifies controls that should be implemented to guarantee sufficient audit records for after the fact investigations and to prove compliancy.

Table 49 Audit capability maturity construction

ILT	AUDIT
A	1. The type of event of users and state of machine regarding security-relevant events are audited. (NIST 3.13.1.1) 2. Audit requirements and activities involving verification of operational systems are carefully planned and agreed upon. (ISO/IEC 12.7.1) 3. Sufficient audit record storage capacity is allocated and configured to prevent exceeding. (NIST AU-4)
B	1. The clocks of information systems or security domains are synchronized to a single reference time source. (ISO/IEC 12.4.4) 2. Audit trail function can be queried for set of parameters to simplify audit trail review easier. (NIST 3.13.3.2) 3. Audit analysis tools developed to reduce the amount of data contained in audit records are used in a real-time. (NIST 3.13.3.5)
C	1. Audit logs provide support for after-the-fact investigations of security incidents and regulations and retention requirements. (NIST AU-11) 2. During audit failure the information system alerts appropriate enterpriseal officials and takes action. (NIST AU-5) 3. The audit trail provides accountability due the tracing of user actions. (NIST 3.13.1)
D	1. Detailed audit logging is enforced for access to nonpublic data. (CIS 14.6) 2. Two synchronized time sources are used for servers and network equipment to synchronize time. (CIS 6.1) 3. The system maintain the identity of all active users internally and is able to link actions to users.(NIST 3.11.1.2)

Log

The capability log defines specific controls that should be implemented to gather logging of specific systems within the network.

Table 50 Log capability maturity construction

ILT	LOG
A	1. All systems storing logs have adequate storage space for daily generated logs. (CIS 6.3) 2. Event logs recording user activities and information security events are produced, kept and regularly reviewed. (ISO/IEC 12.4.1)
B	1. When dynamically assigning addresses using DHCP the dynamic host configuration protocol server logging is deployed. (CIS 1.2) 2. On DMZ networks monitoring systems are configured to record full packet header and payloads of the. (CIS 12.2)
C	1. Network boundary devices are configured to verbosely log all traffic both allowed and blocked arriving at the device. (CIS 6.5) 2. All URL requests from all systems are logged to identify potentially malicious activity and potentially compromised systems. (CIS 7.4)
D	1. Systems are configured to issue a log entry and alert when an account is added to or removed from a system. (CIS 5.4) 2. Systems are configured to issue a log entry and alert on any unsuccessful login to an account. (CIS 5.5)

Manage

The capability manage gaurantees logs and audit trails are managed according to specific predefined procedures.

Table 51 Manage capability maturity construction

ILT	MANAGE
A	1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy (NIST PR.PT-1) 2. A regularly updated audit and accountability policy is used as design foundation and controls are implemented.
B	1. Reviewers know what to look for and are effective in spotting unusual activity. (NIST 3.13.3.1) 2. System administrator and system operator activities are logged, protected and regularly reviewed. (ISO/IEC 12.4.3)
C	1. Based on importance of identifying unauthorized activities managers determine review of audit trail activities. (NIST 3.13.3.4) 2. Security personnel run reports that identify anomalies, actively review the anomalies and documenting their findings. (CIS 6.4)
D	1. Audit log settings for each hardware device and software are validated if specifications in polucy are met. (CIS 6.2) 2. Logging facilities and log information is protected against tampering and unauthorized access. (ISO/IEC 12.4.2)

Monitor

The capability monitor lays down controls in which manner the network should be monitored to detect anomalous activity.

Table 52 Monitor capability maturity construction

ILT	MONITOR
A	1. NetFlow collection is deployed and analysis DMZ network flows to detect anomalous activity. (CIS 12.9) 2. Event data are aggregated and correlated from multiple sources and sensors (NIST DE.AE-3) 3. The use of all accounts is regularly monitored. (CIS 16.4)
B	1. Logs associated with scanning activity and associated administrator accounts are monitored. (CIS 4.6) 2. Attempts to access deactivated accounts is monitor through audit logging. (CIS 16.8) 3. Personnel activity is monitored to detect potential cybersecurity events (NIST DE.CM-3)
C	1. A log analytic tools for log aggregation, consolidation, correlation and analysis is deployed and reports significant alerts. (CIS 6.6) 2. External service provider activity is monitored for potential cybersecurity events (NIST DE.CM-6) 3. Audit trails are designed and implemented to record appropriate information to assist real-time in intrusion detection. (NIST 3.13.3)
D	1. Each user's typical account usage is profiled via normal time-of-day access duration to recognize deviating behaviour. (CIS 16.10) 2. Account usage is monitored to determine dormant accounts, exceptions ar documented and monitored. (CIS 16.6) 3. Configuration monitoring system verify all remotely testable secure configuration elements, and alerts when unauthorized changes occur. (CIS 3.6)

PEOPLE

The FAG People provides controls with regard relevant cybersecurity aspects of human interaction with IT. As well as for Process, measures prescribed by Zero Trust do not comprehend the People aspect of cybersecurity. These measures are created and constructed with Zero Trust in mind.

This group contains FAs:

1. Employee Awareness (EA);
2. Human Resources (HR).

EMPLOYEE AWARENESS (EA)

Making sure that all personnel is conscious regarding the threats and potential consequences they face when using devices, applications or handling information. It is achieved by implementing controls regarding capabilities:

1. Assessment;
2. Awareness;
3. Management;
4. Training.

Assessment

The capability assessment defines controls in which manners the enterprise should assess the readability for when incident scenarios occur.

Table 53 Assessment capability maturity construction

EA	ASSESSMENT
A	1. Periodic incident scenario sessions for personnel associated with the incident handling team are conducted. (CIS 19.7) 2. The extent and frequency of testing varies among systems. (NIST 3.6.5.2)
B	1. Periodic Red Team exercises are performed to test readiness, identification and response. (CIS 20.3) 2. Assessments of the security controls in information systems are conducted to determine correct implementation of controls. (NIST CA-2)
C	1. A mimic of the production environment available for specific penetration tests and Red Team attacks against untested elements. (CIS 20.8) 2. Red Team's results are documented using open, machine-readable standards and a scoring method for the results comparison. (CIS 20.7)
D	1. Contingency and disaster recovery procedures are exercised. (NIST Principle 23) 2. Security skills assessments are used for each of the mission-critical roles to identify skills gaps. (CIS 17.5)

Awareness

The capability awareness lays down controls to inform employees of the current threats that the enterprise faces.

Table 54 Awareness capability maturity construction

EA	AWARENESS
A	1. Users are informed if keystroke monitoring takes place. (NIST 3.13.4.2) 2. A regularly updated security awareness and training policy is used as design foundation and controls are implemented.
B	1. A security awareness program is implemented that focuses on methods via online modules, updates, participation and monitoring. (CIS 17.3) 2. Gap analysis are performed and results are used to build a baseline training and awareness roadmap. (CIS 17.1)
C	1. For all personnel information is published regarding reporting computer anomalies and reported incidents and used in trainings. (CIS 19.6) 2. For administering the program consider visibility, training methods, topics, materials, and presentation techniques. (NIST 3.8.5)
D	1. Awareness levels are validated and improved through periodic tests for social engineering awareness. (CIS 17.4) 2. Employees are aware of threats regarding manipulation, infected websites and use of personal devices. (IASME 4.5.4)

Management

The capability management defines how awareness of employees should be managed to guarantee employees are informed of current threats.

Table 55 Management capability maturity construction

EA	MANAGEMENT
A	1. Information security policy is communicated to all personnel and they are aware of contents and comply. (GAISP 3.2) 2. Support of management and employees for an awareness and training program is achieved. (NIST 3.8.4)
B	1. Individual information system security training activities are documented and monitored. (NIST AT-4) 2. Possible user dissatisfaction is decreased by informing users why that type of authentication is used. (NIST 3.11.4.2)
C	1. There is be a formal and communicated disciplinary process in place to take action against information security breach. (ISO/IEC 7.2.3) 2. Trainers communicate information effectively and have knowledge of the computer security policy implementation. (NIST 3.8.2)
D	1. The missions statement includes computer security program function and responsibilities and related programs and entities. (NIST 3.2.1.3) 2. Retained awareness information, compliance and general attitudes with computer security procedures are evaluated. (NIST 3.8.7)

Training

The capability training specifies in which manner employees should be trained in their security responsibilities

Table 56 Training capability maturity construction

EA	TRAINING
A	1. Users are taught not to use easy-to-guess, not to divulge, and not to store passwords where others can find them. (NIST 3.11.3.3) 2. Training is delivered by fill skills gap, onsite and by senior staff or outside teachers or training conferences or online training. (CIS 17.2)
B	1. All employees are aware of and adequately trained in their security responsibilities. (IASME 4.5.3) 2. Efforts are made to keep abreast of changes in computer technology and security requirements. (NIST 3.8.6)
C	1. Personnel is trained in contingency roles and responsibilities and refresher training is provided. (NIST CP-3) 2. Personnel is trained in incident response roles and responsibilities and refresher training is provided. (NIST IR-2)
D	1. A computer security awareness and training program that distinguishes between groups of people is provided to ensure best results. (NIST 3.8.3) 2. All software development personnel receive training in writing secure code for their specific development environment. (CIS 18.8)

HUMAN RESOURCES (HR)

Controls listed in this focus area provide guidelines which will include cybersecurity in human resources. It is achieved by implementing controls regarding capabilities:

1. Consciousness;
2. Procedures.

Consciousness

The capability consciousness specifies in what extend employees should understand their roles and responsibilities.

Table 57 Consciousness capability maturity construction

HR	CONSCIOUSNESS
A	1. Privileged users understand roles & responsibilities (NIST PR.AT-2) 2. Senior executives understand roles & responsibilities (NIST PR.AT-4)
B	1. Physical and information security personnel understand roles & responsibilities (NIST PR.AT-5) 2. Personnel know their roles and order of operations when a response is needed (NIST RS.CO-1)
C	1. Third-party stakeholders understand roles & responsibilities (NIST PR.AT-3) 2. Information security roles & responsibilities are coordinated and aligned with internal roles and external partners (NIST ID.GV-2)
D	1. The system security managers have security integrated into system management with certain dependencies in place. (NIST 3.2.2.3) 2. Personnel with information security roles are identified, documented, and provide appropriate security training before authorizing access. (NIST AT-3)

Procedures

The capability procedures specifies which procedures should be taken when hiring and firing employees.

Table 58 Procedures capability maturity construction

HR	PROCEDURES
A	1. A regularly updated personnel security policy is used as design foundation and controls are implemented. (NIST PS-1) 2. Qualifications related to integrity, need-to-know, and technical competence are established and verified for all parties. (GAISP 3.6)
B	1. Position sensitivity is determined based on the duties and access levels in order to cost-effectively screen applicants. (NIST 3.5.1.2) 2. Candidates for employment are subjected to background verification checks. (ISO/IEC 7.1.1)
C	1. Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established (NIST ID.AM-6) 2. Appropriate access agreements are completed for individuals requiring access to information systems before authorizing access. (NIST PS-6)

D

1. Conflicting duties and areas of responsibility are segregated to reduce opportunities for mismanagement. (ISO/IEC 6.1.2)
2. Employees are rotated in sensitive positions to prevent internal scams, unauthorized and illegal acts. (NIST 3.5.2.3)

4.3 CHANGES TO FOCUS AREAS

In the first stage of this research project an SLR was executed, the goal of this SLR was to get insight in the principles of Zero Trust. Based on the results of this SLR, which are described in chapter SLR Documentation the base for the focus areas has been created. Additionally, three focus areas are added. During the second stage of this research project a comparison analysis was performed based on guidelines from Becker et al (2009). The comparison analysis resulted in various aspects that should be included in the design of the ZeTuMM, including the focus areas Employee Awareness, Cybersecurity Exercises and Information Sharing. During this stage of the research project the ZeTuMM's focus areas and maturity levels are designed according to guidelines via (Steenbergen et al., 2010) and are outlined in chapter ZeTuMM Description.

synthesization controls in the predefined focus areas, grouping controls in capabilities and creating the maturity constructions within the capabilities, some changes to the focus areas have been made. These changes have been made because controls to implement the concepts and measures, as described in chapter SLR Documentation are the same or are implied. An overview of the changes made is depicted in Table 59.

Table 59 Changes to original defined focus areas

Focus Areas	*Abbr.*	Changes
Permission		*No changes*
~~Application Whitelisting~~	~~AW~~	**Application Whitelisting** has been removed as focus area.
~~Inventory-Based Access Control~~	~~IBAC~~	Controls within this group are moved to **Information System Security** and **Least Privilege & Access Control**.
Ensure Secure Access	ESA	Capability Functional and Authenticate (1/3) from **Application Whitelisting** has been added. Added to group **Permission,** since controls prescribe more in which manner access is granted
Information System Security	ISS	Newly created focus area, the goal of **Information System Security** is to manage security of an Information System. This focus area is composited of: - Capability Physical (1/3) within **Application Whitelisting** - Capability Compliancy (1/2) within **Inventory-Based Access Control** - Capability Logical (1/1) within **Securely Identifying the Device**
Least Privilege & Access Control	LPAC	Capability Access Control (1/2) within **Inventory-Based Access Control** has been added.
~~**Network**~~ **Infrastructure**		Changed focus area group name **Network** to **Infrastructure**, since focus areas in this group are not only applicable to the network
~~Central Management~~	~~CM~~	**Central Management** has been removed as focus area. Various controls prescribe **Central Management** of people, processes and techniques, but these controls fitted better in other groups.
~~Control Shadow IT~~	~~CSIT~~	**Control Shadow IT** was removed as Focus Area.

		Controls within this group are similar to controls from groups **Securely Identify Device** and **Ensure Secure Access**.
~~Securely Identifying Device~~ IT Life-Cycle	~~SID~~ ITLC	Securely identifying Device has been moved to **Infrastructure** and renamed to IT Life-Cycle. Capability Maintenance (1/3) within **Application Whitelisting** has been added.
~~Data Abstraction~~	~~DA~~	Data Abstraction has been removed as Focus Area.
Data Life-Cycle	DLC	Capabilities Technique and Encryption (2/2) within **Data Abstraction** were added Added to group **Infrastructure,** since controls within Data Life-Cycle are controls which should be implemented on systems or network.
Information System Life-Cycle	ISLC	Newly created focus area, this focus area contains controls to manage the information system's life-cycle.
Network Segmentation	NS	Capability Unprivileged (1/1) from **Unprivileged Network** were added
~~Parallelize Switching Cores~~	~~PSC~~	Parallelize Switching Cores has been removed as focus area The synthesization did not yield any **Parallelize Switching Cores** controls. A couple of controls implied the criteria, but clearly belonged in focus area Network Segmentation.
Processes		*No Changes*
Contingency Management	CM	Newly created focus area, **Contingency Management** is combined out of capabilities that will manage unexpected events by providing controls that provide operational continuity
Incident Management	IM	*No changes*
Enterpriseal Management	OM	Newly created focus area, the goal of **Enterpriseal Management** is to provide an enterprise controls to manage and protect the enterprise
Risk Management	RM	Newly created focus area, **Risk Management** hosts capabilities to identify, analyze and control risk to mitigate potential damages of potentially unfortunate expected events
Intelligence		*No changes*
Advanced Threat Protection	ATP	The capability Sharing (1/1) within **Information Sharing** has been added.
~~Cloud Visibility~~	~~CV~~	**Cloud Visibility** has been removed as focus area. The goal of this model is to provide sound security measures so company can improve their security, with only three measures for cloud security, this capability should not be included.
~~Information Sharing~~	~~IS~~	**Information sharing** has been removed as focus area.
Inspect & Log Traffic	ILT	*No changes*
People		*No changes*
~~Cybersecurity Exercises~~	~~CE~~	**Cybersecurity Exercises** has been removed as focus area.

Employee Awareness	EA	Capability Assessment (1/1) within **Cybersecurity Exercises** has been added
Human Resources	HR	Newly created focus area, controls listed in **Human Resources** provide guidelines which will include cybersecurity in human resource management.

The preceding changes, synthesization and maturity construction activities have resulted in the skeleton of ZeTuMM. The model that consists out of five focus area groups, the five focus area groups have fifteen focus areas defined, these fifteen focus areas have 57 capabilities, the 57 capabilities each have four maturity stages and the maturity levels can exist out of four to twelve controls. In total the model and harbor 460 cybersecurity controls. Depicted in Table 60 are the amount of controls per capability, per focus areas and per focus area goups, capabilities are grouped per focus area and focus area per focus area group.

Table 60 Overview of capabilities within focus areas within focus area goups

Names	#	Names	#	Names	#	Names	#
Permission	64	Infrastructure	136	Processes	132	Intelligence	72
ESA	***16***	***CSIT***	***32***	***CM***	***32***	***ATP***	***32***
Authentication	8	Asset	8	Assurance	8	Detection	8
Device	8	Configuration	8	Capacity	8	Management	8
ISS	***32***	Maintenance	8	Environmental	8	Prevent	8
Condition	*8*	Management	8	Planning	8	Sharing	8
Governance	8	***DLC***	***40***	***IM***	***32***	***ILT***	***40***
Logical	8	Encryption	8	Management	8	Audit	12
Physical	8	Identification	8	Report	8	Log	8
LPAC	***16***	Prevention	8	Resolve	8	Manage	8
Accounts	8	Protection	8	Response	8	Monitor	12
Controls	8	Technique	8	***OM***	***36***	People	48
		ISLC	***24***	Physical	8	***EA***	***32***
		Acquisition	8	Policy	8	Assessment	8
		Development	8	Procedure	8	Awareness	8
		Management	8	Roadmap	12	Management	8
		NS	***40***	***RM***	***32***	Training	8
		Connections	8	Analyze	8	***HR***	***16***
		Filtering	8	Back-up	8	Consciousness	8
		Segmentation	8	Control	8	Procedures	8
		Segregation	8	Identify	8	Procedures	8
		Unprivileged	8				

4.4 TOOLS

To calculate the maturity of a company, the ZeTuMM uses various calculations to give a representation of a company's maturity. On top of these calculations, specific diagrams are used to provide a graphical view. This chapter explains how the calculations work and which diagrams are used.

ATTAINED MATURITY LEVEL CALCULATIONS

Results of the Maturity Model are two-folded; the maturity model uses two calculation techniques. The first calculation of the model measures the Zero Trust maturity. Zero Trust maturity measurements are strict – before you go to the next maturity level – every control within a specific maturity level needs to be implemented. Another important aspect is that you always start in level 1.

Figure 18 is used as an example. Capability Account is constructed from eight control questions (like most capabilities are). Within the Zero Trust maturity one always starts in level 1. To get to the second level, control question A.1 and A.2 needs to be answered with 'Yes'. In Figure 18 control questions A.1, A.2, B.1 and B.2 are answered with Yes, this means that level 3 is accomplished.

ML	Least Privilege & Access Control	Account	Completed	Answer	ICa
A.1	Are processes established for requesting, establishing, issuing, and closing user accounts?			Yes	1
A.2	Are users required to change their passwords periodically?			Yes	1
B.1	Are accounts locked after various failed login attempts?			Yes	1
B.2	Are secure password attributes specified and required?			Yes	1
C.1	Are administrative accounts automatically inventoried and privileges validated?			No	0
C.2	Are user IDs that have been inactive on the system for a specific period of time disabled?			No	0
D.1	Is acces to an accounts that is specifically used for task like transactions, pentesting or others only granted for the duration of that task?			No	0
D.2	Are activities with respect to the enforcement and usage of users information system access controls supervised and reviewerd?			No	0

Figure 18 Example Capability Account

In some cases, it can be that seven control questions are answered with 'Yes', but the maturity level is still level 1. This is when control question A.1 or A.2 is answered with 'No'. In this case, the results will be distorted, for this reason the model makes use of a second maturity measurement. This measurement measures the amount of controls implemented: every control has the same weight. An example for this can be seen in Figure 19.

ML	Least Privilege & Access Control	Control	Completed	Answer	ICa
A.1	Is an access control policy developed, documentend, regularly updated, disseminated and used as design foundation to facilitate correct control implementation?			Yes	1
A.2	Are access permissions managed, incorporating the principles of least privilege and separation of duties?			No	0.5
B.1	Are access control lists implemented for authorization to use system resources?			Yes	1
B.2	Are audit information and audit tools protected from unauthorized access, modification, and deletion?			Yes	1
C.1	Is unauthorized access to information in printed form and/or removable media prevented ?			Yes	1
C.2	Is access controlled by a secure log-on procedure where required by the access control policy?			Yes	1
D.1	Is access to system files and source code controlled?			Yes	1
D.2	Are types of access, or access modes considered?			Yes	1

Figure 19 Example Capability Control

Since control A.2 is not fully implemented, the Zero Trust maturity is level 1. Here comes the second measurement in hands. A.2 is not fully implemented, only the separation of duties is applied. In total 7,5 of 8 controls are implemented, which gives 93,75% of implemented controls. So, the results of Capability Control is Zero Trust maturity level 1 with 93,75% implemented controls.

It could be that a control or capability is Not Applicable (N/A). For Zero Trust maturity measurement a Not Applicable is calculated as a 'Yes'. For Example: if A.2 in Figure 19 would be a 'N/A', then the Zero Trust Maturity would be level 5, with seven out of seven - or 100% - controls implemented.

Focus Area (Group) Maturity

As explained earlier in this document, Capabilities are grouped in Focus Areas (FAs) and FAs are grouped in a Focus Area Groups (FAGs). Measuring the Zero Trust maturity within the FA as well as in the FAG is done in a similar manner. The maturity of a FA is defined by the lowest maturity of one of the Capabilities within the group. This also goes for the FAG, where the maturity is defined by the lowest Zero Trust maturity of a FA.

For example: FA Least Privilege & Access Control has two Capabilities, these are Account and Control. When Capability Account is on level 3, but Control is on level 1, the overall Zero Trust maturity of the FA Least Privilege & Access Control is level 1. Then again for the Focus Area Group Permission, which includes the Focus Area Least Privilege & Access Control, will have level 1 as Zero Trust Maturity. For this reason, all the results in this document will depict the second maturity measurement, which calculates the percentage of total implemented controls relative to the applicable controls (total controls minus the N/A controls).

Additional Graphical Representations

The Zero Trust Maturity Model provides various graphical representations of the results. These graphical representations are created based on the answers provided in the maturity model and are provided in the Focus Area Group, Focus Area and Capability views.

Attained Maturity vs Implemented Controls

This graph depicts the maturity level values of the pre-defined focus area groups of the Zero Trust Maturity Model in combination with a secondary calculation method that calculates the % of implemented controls.

ACCUMULATION MATURITY LEVELS

This graph displays the attained maturity levels of the fifteen focus areas that the model uses. Maturity levels are denoted as N/A, A, B, C and D. N/A means there are no controls according to Zero Trust implemented.

ACCUMULATION CONTROLS AND STATUS

To provide insight regarding the amount of controls that could be implemented and/or are implemented, this graph displays the amount of Effective Controls, Implemented Controls and the remaining accomplishable Controls.

ACCUMULATION MATURITY STAGES PER MATURITY LEVEL

This graph provides insight regarding the amount of controls that are implemented, initiated, applicable and not applicable per Maturity Level.

ACCUMULATION ATTAINED MATURITY LEVELS AND STAGES

This graph displays the amount of maturity levels which are attained or are not applicable. It also provides an overview of the extent of maturity stages that are fully implemented or that at least has one control implemented.

OVERALL ATTAINED MATURITY VS IMPLEMENTED CONTROLS

The overall score of the assessment is depicted in this bar chart.

OVERALL ACCUMULATION CONTROLS AND STATUS

The graph stated above displays the overall status of all controls that are used for the maturity measurement.

5 Case Study Validation

The goals of the case study are two-folded. On the one hand, I will use the interactions to improve the model, I expect to hear feedback regarding the maturity constructions which are used in this maturity model. On the other hand, the case study participants can use the results to improve the state of security corporate-wide. This is achieved by knowing what the security strengths are. Based on these strengths, improvement areas are selected to create a security improvement strategy. Time and duration of the interview depends on the number of questions. It will vary between 30 to 60 seconds to ask and answer a question. For each interview, seven minutes are used for introduction.

After completion of the case study results of ZeTuMM are analyzed. To guarantee solid cybersecurity advice after analyzation, this activity is divided in three consecutive stages. Firstly, results will be analyzed to identify strengths and improvement areas. During this stage, the person of contact will be informed when formal advice can be expected based on initial findings. Secondly, results of the assessment will be provided in an advice report. This report focusses on cybersecurity strengths, based on these strengths improvement areas are selected. Finally, gained feedback from the interviews and the results to find opportunities to improve the model and create a final version of the ZeTuMM.

In total, the Case Study is held by three enterprises at three different branches. As the model is created out of a modular construction, it was important to find enterprises that deal with all the focus area group security metrics. The two of the selected companies used all the focus areas in their security. One enterprise lacked one focus area, that was focus area development. All enterprises was promised anonymity, so the companies are referred as enterprise A, B and C.

Before the first case study was held, two cybersecurity experts reviewed the model. Reviewer A is a medior cyber security consultant with over 5 years of experience in the field. Reviewer B is a senior zero trust cyber security consultant with over 10 years of experience. As botch consultants followed my research, they were closely involved in the development of the model.

5.1 ENTERPRISE A

Enterprise A is a consultancy and security delivery enterprise. The enterprise is highly specialized in Zero Trust security.

Employees:	35
Interviewees:	1
Type:	Consultancy
Located:	National

This chapter is made up of:

1. Interviewee;
2. Results;
3. Advice.

INTERVIEWEE

RESULTS

ADVICE

5.2 ENTERPRISE B

Enterprise B is an agricultural company. The company develops its own software for the management of livestock and is one of the leading companies in their field. Due to some limitations only, questions of FAG Permission and Intelligence were answered.

Employees:	1300
Interviewees:	3
Type:	Agriculture
Location:	International

This chapter is made up of:

1. Interviewee;
2. Results;
3. Advice.

INTERVIEWEE

RESULTS

ADVICE

5.3 ENTERPRISE C

Enterprise C is a technological company. The company is leading in its technologies field. The company employs tens of thousands of people all over the world. The case study interview was conducted with seven employees.

Employees:	17.000

Interviewees:	7
Type:	Technology
Location:	International

This chapter provides:

1. Interviewees
2. Results;
3. Advice.

INTERVIEWEES

RESULTS

ADVICE

6 CONCLUSION

This chapter describes the conclusions that are drawn from this research and contains the following paragraphs:

1. Discussion;
2. Future Research;
3. Conclusion.

6.1 DISCUSSION

Even though various research about cybersecurity is executed, the clear majority focusses on the Trust but Verify principles. It was hard finding the right scientific papers and research that are published regarding the Zero Trust Principle. It can be argued that not all scientific papers are of the best quality. Many papers cite also one and another. This all had the result that I was not able to find any maturity models with the Zero Trust principle in mind. With the use of SLR, comparison analysis, maturity modeling comparison, I think this research is a solid aggregation of the science regarding the Zero Trust principles.

The construction of the maturity model was a difficult aspect. Most research that I harvested from the SLR is written by John Kindervag. John Kindervag writes his theories in a prescriptive manner and not all techniques that he describes – regarding the construction of Zero Trust Architectures – are available as products for companies that wish to implement Zero Trust. On top of that, most cybersecurity framework do not possess such technical controls. This resulted in a gap between the theoretical aspects of Zero Trust and existing cybersecurity controls from widely used cybersecurity frameworks. With experience and the help from experts in the fields I was able to group these Controls in capabilities, that are grouped in focus areas and these focus areas are grouped in focus area groups.

A missing aspect in the maturity model can be found when enterprises outsource aspects of their IT infrastructure or IT development. The frameworks that are used in the creation of this maturity model only had limited controls regarding outsourcing aspects of IT. For this reason, I excluded a few controls that covered this aspect, mostly because I felt that these controls were not sufficient to cover outsourcing aspects regarding cybersecurity. This decision was supported by the experts that were involved in this research.

Even though the model was validated in three different companies that differ in size and private sector, it would provide a higher validation maturity if more companies would be willing to participate in the case study. Nonetheless, the case study at the companies that participated were a success. The maturity model covered all aspects of their cybersecurity practices and they all found the results helpful to further improve their maturity in cybersecurity.

6.2 FUTURE RESEARCH

For further research it is recommended that more research regarding Zero Trust is carried out. Google is one of the companies that is leading with the implementation of Zero Trust Architectures. It would be highly interesting to perform a case study at Google and further advance the model. Another addition to the model would be the inclusion of cybersecurity controls for outsourcing IT infrastructures and mobile security. These aspects are currently lacking in this model.

During the development and validation of the model, aspects regarding the grouping of controls arose. It would be highly interesting to research aspects about how the weight of controls can be measured. Depending on the types of IT infrastructure of companies, the effect of implementation of certain controls have a higher impact on the state of cybersecurity than others. This 'weight' would be highly dynamic, it would be a challenge to come up with a solution to define metrics that solve this dynamic aspect of the impact of cybersecurity controls.

In 2017 the O-ISM3 maturity model was released by The Open Group. Unfortunately, this was after I completed my Maturity Model Analysis. For future work is would also be interesting to compare the ZeTuMM against the O-ISM3.

6.3 CONCLUSION

The goal of this research is to find a manner how enterprises can let go of the Trust but Verify principle and embrace the Zero Trust principle to keep their complex network secure. To reach this goal the following sub-research questions (SQ) are defined:

> **SQ1:** *"What is known about cybersecurity related to the Zero Trust principle?"*

To answer this sub-research question, an extensive SLR is performed to harvest the existing research regarding the Zero Trust principle. With the use of a predefined search string in Google Scholar and Scopus twelve scientific papers are defined. From these papers it can be concluded that Zero Trust has certain concepts and measures. The concepts are principles regarding the design of a Zero Trust Architecture. The measures found in the papers are more concrete cybersecurity solution and techniques that can be implemented. In total Zero Trust has three concepts and thirteen measures.

> **SQ2: "***Can existing cybersecurity (maturity) models be used in creation of a Zero Trust Maturity Model?"*

Since many cybersecurity maturity models were created before the start of this research, this sub-research question is formulated to research whether (parts of) existing maturity model can be reused in the creation of the maturity model. With the use of the SLR technique and predefined search string in Google Scholar and Scopus, with results set from 2010 an onwards – to guarantee relevancy-, a total of eight maturity models were found. After comparing the maturity models on the way they were created and defining strong aspects of these models, it is concluded that these model contain eight characteristics that are reused within the creation of the ZeTuMM.

> **SQ3: "***Which focus areas and maturity levels need to be defined to create the Zero Trust Focus Area Maturity Model?"*

With controls harvested from eight widely used frameworks in the cybersecurity community and the research that is executed on Zero Trust literature, a total of fifteen focus areas are defined. The fifteen focus areas are grouped in five logical focus area groups. The focus areas contains 53 capabilities. Each capability has five maturity levels and consists out of eight cybersecurity controls. In total 428 are classified within the maturity levels within the capabilities. Various controls have elemental dependencies, of which some controls regarding policy have multiple. Based on the size of an enterprise, enterprise infrastructure and IT management strategies, it can be decided that specific capabilities and controls, up to entire focus areas, are not applicable.

SQ4: *"Is it possible to measure objectively the maturity of enterprises in the Zero Trust Focus Area Maturity Model?"*

All the 428 cybersecurity descriptive controls used in the model are rephrased to yes or no questions. It is also possible to provide a Not Applicable (N/A) answers, since a control can be not applicable within an enterprise. By enforcing yes or no answers during the maturity assessment and by giving all the cybersecurity controls the same weight, an objective representation about the state of cybersecurity is the result.

SQ5: *"Which controls have Dutch enterprises used to comply with cyber security in the Zero Trust principle?"*

Since the controls used in the ZeTuMM are harvested from widely used cybersecurity frameworks, it is to be expected that enterprises implemented various controls. After the case studies this expectation is confirmed. The highest implementation rate of controls was 88%, followed by 73% and the third enterprise had 46% of the controls implemented. Maturity levels regarding the Process are on the highest levels, one enterprise had almost all controls regarding the processes implemented. Controls regarding Permissions and Infrastructure were least implemented. Even though these high implementation rate, the maturity levels in the enterprises were not that high at all. This is mainly because basic controls – that take in account the three Zero Trust concepts – were not implemented, but others were.

With the answers of preceding sub-research questions, the main research question can be answered. The main research question aims to answer the way in which enterprises can close the gap between the Trust but Verify and Zero Trust cybersecurity maturity. The following research question is formulated:

RQ: *In which manner can enterprises improve their cybersecurity maturity in the Zero Trust principle?*

The Zero Trust Maturity Model is proven to be a way in which enterprises can improve their cybersecurity. Enterprises can do this by executing the Zero Trust Maturity Model Assessment. The results of this assessment provide insight in the state of Zero Trust implementation within an enterprise. With these insights an enterprise can define which cybersecurity controls should be implemented and create a roadmap to improve the cybersecurity maturity in the Zero Trust Principle.

REFERENCES

AIVD, GOVCERT.NL, KLPD, MIVD, Nct. en O. (2010). Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308–313. http://doi.org/10.1016/S0167-4048(03)00407-3

Anderson, R., & Moore, T. (2006). The economics of information security. *Science (New York, N.Y.)*, *314*(5799), 610–613. http://doi.org/10.1126/science.1130992

Balaouras, S., Kindervag, J., Holland, R., & Shey, H. (2014). *Defend your data From Mutating Threats With a Zero Trust Network*.

Banafa, A. (2014). *What is zero trust model of information security ?*

Barlette, Y., & Fomin, V. (2010). The Adoption of Information Security Management Standards. *Information Resources Management: …*, 119–140. Retrieved from http://books.google.es/books?hl=en&lr=&id=zIdVXq5BLOMC&oi=fnd&pg=PA69&dq=(%22paper+computing%22+OR+%22augmented+paper%22)+AND+(education)+AND+(classroom+OR+school+OR+university)&ots=RfLaKAnL8D&sig=T0ILUqZBdQViG1aQTqrPCuYGNCo

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*. http://doi.org/10.1007/s12599-009-0044-5

Bowen, P., & Kissel, R. (2007). NISTIR 7358: Program Review for Information Security Management Assistance (PRISMA), 1–60.

Brereton, P., Kitchenham, B. a., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583. http://doi.org/10.1016/j.jss.2006.07.009

Brummelkamp, G. (2009). *Criminaliteitspreventie door kleine bedrijven*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Emperical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, (34.3), 523–548. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2919&context=misq

Carin, L., Cybenko, G., & Hughes, J. (2008). Cybersecurity strategies: The queries methodology. *Computer*, 20–26. Retrieved from https://securitymetrics.org/attachments/Metricon-3-Cybenko-Article.pdf

CIS, C. for I. S. (2014). The CIS critical security controls for effective cyber defense, 106.

Coelho, R. W., Jr, G. F., Lemes, M., & Jr, P. (2014). GAIA-MLIS : A Maturity Model for Information Security. *SECURWARE 2014*, (61), 50–55.

Consortium, I. (2007). *Information Security Management Maturity Model version 2.10*.

CSIS, & McAfee. (2014). Net Losses : Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, (June).

Denning, D. (2000). Information Warfare And Security. *Edpacs*, *27*(9), 1–2. http://doi.org/10.1201/1079/43255.27.9.20000301/30321.7

Dhillon, H., & Hentea, M. (2005). Getting a cybersecurity program started on low budget. *Proceedings of the 43rd Annual Southeast Regional Conference*, *1*(ACM).

Dimopoulos, V., Furnell, S., Jennex, M., & Kritharas, I. (2004). Approaches to IT Security in Small and

Medium Enterprises. In *AISM* (pp. 73–82). Retrieved from http://igneous.scis.ecu.edu.au/proceedings/2004/aism/InfoSec Conference Complete Proceedings.pdf#page=83

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia. *ECIS*, 1560–1571. Retrieved from http://dro.deakin.edu.au/view/DU:30008152

Duff, A. (1996). The literature search : a library-based model for. *Library Review*, *45*(4), 14–18.

Dyn. (2014). *Everything you need to know about a ddos attack*. Retrieved from file:///C:/Users/Michel/Downloads/w_dyni35.pdf

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) enterprises. *Government Information Quarterly*, *26*(4), 584–593. http://doi.org/10.1016/j.giq.2009.04.004

Fenz, S., & Ekelhart, A. (2009). Formalizing information security knowledge. *… 4th International Symposium on Information …*, 183. http://doi.org/10.1145/1533057.1533084

Fenz, S., Neubauer, T., Accorsi, R., & Koslowski, T. (2013). FORISK: Formalizing information security risk and compliance management. *Proceedings of the International Conference on Dependable Systems and Networks*. http://doi.org/10.1109/DSNW.2013.6615533

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*, *23*(4), 367–376. http://doi.org/10.1108/17542731111139455

GOVCERT.nl. (2007). Trendrapport 2007.

GOVCERT.nl. (2008). Trendrapport 2008.

GOVCERT.nl. (2009). Trendrapport 2009.

Hahn, A., Ashok, A., Sridhar, S., & Govindarasu, M. (2013). Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid*, *4*(2), 847–855. http://doi.org/10.1109/TSG.2012.2226919

Humphrey, W. S. (1989). *Managing the Software Process*. (N. Habermann, Ed.), *OMEGAINTERNATIONAL JOURNAL OF MANAGEMENT SCIENCE* (Vol. 16). Addison-Wesley Professional.

Iankoulova, I., & Daneva, M. (2012). Cloud computing security requirements: A systematic review. *Research Challenges in Information Science (RCIS)*, *IEEE*(2012 Sixth International Conference), 1–7. http://doi.org/10.1109/RCIS.2012.6240421

IASME Consortium. (2015). the Standard for Information Assurance for Small and Medium Sized (Iasme), (3).

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*.

ISC2. (2011). CISSP - Certified Information Systems Security Professional | $(ISC)^2$. Retrieved February 24, 2016, from https://www.isc2.org/cissp/default.aspx

ISO. (2005a). *ISO/IEC 27001:2005; Information technology -- Security techniques -- Information security management systems -- Requirements*.

ISO. (2005b). *ISO/IEC 27002:2005; Information technology -- Security techniques -- Code of practice for information security management*.

ISO. (2013). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Code of practice for information security controls, *2013*.

ISSA, I. S. S. A. (2003). Generally Accepted Information Security Principles.

ITU. (2008). X.1205 : Overview of cybersecurity.

Jansen, A. J. (2014). *The Cyber Security Risk Assessment Maturity of Hospitals*.

Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards An Information Security Maturity Model for Secure e-Government Services : A Stakeholders View. *Proceedings of the 5th HAISA2011 Conference*, (58–73), 12. http://doi.org/urn:nbn:se:su:diva-67206

Kindervag, J. (2010a). *Build Security Into Your Network ' s DNA : The Zero Trust Network Architecture*.

Kindervag, J. (2010b). *No More Chewy Centers : Introducing The Zero Trust Model Of Information Security*.

Kindervag, J., Balaouras, S., Holland, R., & Blackborow, J. (2015). Five Steps To A Zero Trust Network.

Kindervag, J., Ferrara, E., Holland, R., & Shey, H. (2013). The National Institute of Science and Technology: Developing a Framework to Improve Critical Infrastructure, (The National Institute of Science and Technology (NIST) within the Department of Commerce (Commerce)), 1–18.

Kindervag, J., Shey, H., & Mak, K. (2014). *The future of data security: A zero trust approach*.

Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud Computing Risk Assessment: A Systematic Literature Review. *Future Information Technology*, (Springer Berlin Heidelberg), 285–295.

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). CYBERSECURITY INFORMATION SHARING: A FRAMEWORK FOR SUSTAINABLE INFORMATION SECURITY MANAGEMENT IN UK SME SUPPLY CHAINS. *ECIS 2014 Proceedings*. Retrieved from http://aisel.aisnet.org/ecis2014/proceedings/track14/4

Moore, A. P., Ellison, R. J., & Linger, R. C. (2001). *Attack Modeling for Information Survivability*. *No. CMU-SEI-2001-TN-001. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST*.

NCSC. (2011). Cybersecuritybeeld Nederland: 2011, (December).

NCSC. (2012). Cybersecuritybeeld Nederland: CSBN-2.

NCSC. (2013). Cybersecuritybeeld Nederland: CSBN-3.

NCSC. (2014). Cybersecuritybeeld Nederland: CSBN-4.

NIST. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems*. *Work*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

NIST. (2004). Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A NIST Special Publication 800-27 Rev A Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A. *NIST Special Publication 800-27 Rev A*, 35.

NIST. (2006). Minimum Security Requirements for Federal Information and Information Systems, NIST Special Publication 800-53. *Information Security*, *March 2006*(March). Retrieved from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

NIST. (2013). *Developing a Framework to Improve Critical Infrastructure Cybersecurity*.

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of S*, 1–41. http://doi.org/10.1109/JPROC.2011.2165269

Palo Alto. (2014). *Getting Started With a Zero Trust Approach to Network Security*.

Palo Alto. (2015). *Zero Trust on the Endpoint Extending the Zero Trust Model from Network to Endpoint with Advanced Endpoint Protection*.

Patsis, M. G. (2007). ENISA Deliverable : Information Package for SMEs With examples of Risk Assessment / Risk Management for two SMEs. *Security*, (February).

Putri, N. R., & Mganga, M. C. (2011). Enhancing Information Security in Cloud Computing Services using SLA Based Metrics. *Blekinge Institute of Technology*, (January), 1–75.

PWC. (2014). *Managing cyber risks in an interconnected world; Key findings from The Global State of Information Security® Survey 2015*. Retrieved from file:///D:/W81PMichel/Downloads/pwc-global-state-of-information-security-survey-20 (1).pdf

Rabai, L. B. A., Jouini, M., Aissa, A. Ben, & Mili, A. (2012). A cybersecurity model in cloud computing environments. *Journal of King Saud University - Computer and Information Sciences*, *25*(1), 63–75. http://doi.org/10.1016/j.jksuci.2012.06.002

Rahim, N. H. A., Hamid, S., Mat Kiah, M. L., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4).

Rebollo, O., Mellado, D., & Fernández-Medina, E. (2012). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *Journal of Universal Computer Science*, *18*(6), 798–815. http://doi.org/10.3217/jucs-018-06-0798

RT. (2014). Security firm says Sony hack might have been an inside job — RT USA. Retrieved January 11, 2015, from http://rt.com/usa/217495-sony-hack-fbi-north-korea/

Saleh, M. (2011). Information Security Maturity Model. *International Journal of Computer Science and Security …*, (5), 316–337. http://doi.org/10.5329/RESI.2013.1201003

Sangani, N., & Vijayakumar, B. (2012). Cyber Security Scenarios and Control for Small and Medium Enterprises. *Informatica Economica*, *16*(2), 58–71. Retrieved from http://revistaie.ase.ro/content/62/07 - Sangani.pdf

Scheerder, J. (2013). *ZeroTrust Networking*.

Shirtz, D., & Elovici, Y. (2011). Optimizing investment decisions in selecting information security remedies. *Information Management & Computer Security*, *19*(2), 95–112. http://doi.org/10.1108/09685221111143042

Silva, L., Paula Costa, A., Poleto, T., & Moura, J. (2012). An analysis of and perspective on the information security maturity model: A case study of a public and a private sector company. *18th Americas Conference on Information Systems 2012, AMCIS 2012*, *3*, 1684–1694. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84877900271&partnerID=40&md5=8f49573949a5275e134734d71b992e6f

Sivaraman, R. (2015). *Zero Trust Security Model*. http://doi.org/10.13140/RG.2.1.4861.9045

Solis, B. (2015). Disruptive Technology Trends 2015 - 2016. Retrieved January 7, 2015, from https://www.linkedin.com/pulse/25-technology-trends-2015-2016-brian-solis

Speer, D. L. (2000). Redefining borders: The challenges of cybercrime. *Crime, Law and Social Change*, *34*(3), 259–273. http://doi.org/10.1023/A:1008332132218

Spruit, M., & Roeling, M. (2014). ISFAM: the Information Security Focus Area Maturity Model, 0–15.

Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I. van de, & Bekkers, W. (2010). The Design of Focus Area Maturity Models. In *Global Perspectives on Design Science Research* (Vol. 6105, pp. 317–332). http://doi.org/10.1007/978-3-642-13335-0_22

Syntens. (2006). *MKB-experiment m.b.t. cybercrime in Flevoland*. Retrieved from http://www.mkb.nl/download.php?itemID=442873

Ten, C. W., Manimaran, G., & Liu, C. C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, *40*(4), 853–865. http://doi.org/10.1109/TSMCA.2010.2048028

van de Weerd, I., & Brinkkemper, S. (2008). Meta-Modeling for Situational Analysis and Design Methods. *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications*, 35–54. http://doi.org/10.4018/978-1-59904-887-1

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers and Security*, *23*(5), 371–376. http://doi.org/10.1016/j.cose.2004.05.002

von Solms, S. B. (2010). The 5 Waves of Information Security – From Kristian Beckman to the Present. *Security and Privacy–Silver Linings in the Cloud.*, *Springer B*, 1–8. Retrieved from http://download-v2.springer.com/static/pdf/45/chp%253A10.1007%252F978-3-642-15257-3_1.pdf?token2=exp=1430811210~acl=%2Fstatic%2Fpdf%2F45%2Fchp%25253A10.1007%25252F978-3-642-15257-3_1.pdf*~hmac=4a8cdc8aed60c19a4afa1b49531969876ef6a0ee08b0ea07c313a4e5c69382

Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. *Usenix Login*, *39*(6), 6–11.

White, G. B. (2011). The community cyber security maturity model. *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 173–178. http://doi.org/10.1109/THS.2011.6107866

Whitman, B. M. E. (2003). ENEMY AT THE GATE: THREATS TO INFORMATION SECURITY. *Communications of the ACM*, *46*(8), 91–95. Retrieved from http://portal.acm.org/citation.cfm?id=859675

Whitman, M., & Mattord, H. (2011). *Principles of Information Security*. Retrieved from https://books.google.com/books?hl=nl&lr=&id=L3LtJAxcsmMC&pgis=1

Xiao-yan, G., Yu-qing, Y., & Li-lei, L. (2011). An Information Security Maturity Evaluation Mode. *Procedia Engineering*, *24*, 335–339. http://doi.org/10.1016/j.proeng.2011.11.2652